February 10, 2011

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: North American Electric Reliability Corporation, Docket No. RM06-22-000

Dear Ms. Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits this petition in accordance with Section 215(d)(1) of the Federal Power Act ("FPA") and Part 39.5 of the Federal Energy Regulatory Commission's ("FERC") regulations and in compliance with directives in FERC Order No. 706[1] seeking approval of the following proposed Critical Infrastructure Protection (CIP) Reliability Standards set forth as **Exhibit A** to this petition:

- CIP-002-4– Cyber Security — Critical Cyber Asset Identification (CIP-002-4)
- CIP-003-4 – Cyber Security — Security Management Controls (CIP-003-4)
- CIP-004-4 – Cyber Security — Personnel & Training (CIP-004-4)
- CIP-005-4 – Cyber Security — Electronic Security Perimeter(s) (CIP-005-4)
- CIP-006-4 – Cyber Security — Physical Security of Critical Cyber Assets (CIP-006-4)
- CIP-007-4 – Cyber Security — Systems Security Management (CIP-007-4)
- CIP-008-4 – Cyber Security — Incident Reporting and Response Planning (CIP-008-4)
- CIP-009-4 – Cyber Security — Recovery Plans for Critical Cyber Assets (CIP-009-4).

These proposed reliability standards were approved by the NERC Board of Trustees on January 24, 2011.

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection.* 122 FERC ¶ 61,040. (2008) (Docket No. RM06-22-000 (Order No. 706)

Additionally, NERC requests FERC approval for the associated implementation plans for CIP-002-4 through CIP-009-4 that call for the retirement of CIP-002-3 through CIP-009-3 and a new effective date that will be determined in accordance with FERC approval of the proposed standards and the Implementation Plan included in **Exhibit B** of this filing.

This filing discusses the proposed CIP Reliability Standards, including how the proposed standards and associated implementation plans meet the criteria identified by FERC in Order No. 672[2] for approving Reliability Standards.

This filing consists of the following:

- This transmittal letter;
- A table of contents;
- A narrative description explaining how the proposed CIP Reliability Standards meet FERC's requirements;
- The proposed CIP Reliability Standards submitted for approval (**Exhibit A**);
- The associated Implementation Plan for the proposed CIP Reliability Standards submitted for approval (**Exhibit B**);
- The associated Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the proposed CIP Reliability Standards submitted for approval (**Exhibit C**);
- The Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706 (**Exhibit D**);
- The Development Record of the proposed CIP Reliability Standards and the associated Implementation Plan (**Exhibit E**); and
- A table of proposed CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval (**Exhibit F**).

[2] *See, Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, FERC Stats. & Regs.*, ¶ 31,204 at PP 320-338 ("Order No. 672"), *order on reh'g*, FERC Stats. & Regs. ¶ 31,212 (2006) ("Order No. 672-A").

Please contact me if you have any questions regarding this filing.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**) Docket No. RM06-22-000)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION (CIP) RELIABILITY STANDARDS VERSION 4

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

February 10, 2011

TABLE OF CONTENTS

I. Introduction 1

II. Notices and Communications 2

III. Background: 2

a. Regulatory Framework 2

b. Basis for Approval of Proposed Reliability Standard 3

c. Reliability Standards Development Procedure 4

IV. Justification for Approval of the Proposed Reliability Standard 7

a. Section Overview 7

b. Demonstration that the proposed Reliability Standard is Just, Reasonable, not Unduly Discriminatory or Preferential, and In The Public Interest 32

c. Violation Risk Factor and Violation Severity Level Assignments 45

V. Summary of the Reliability Standard Development Proceedings 47

a. Development History 47

VI. Conclusion 49

Exhibit A — Proposed CIP Reliability Standards submitted for approval

Exhibit B — Implementation Plan for CIP Reliability Standards submitted for approval

Exhibit C — Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for CIP Reliability Standards submitted for approval

Exhibit D — Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706

Exhibit E — Development Record of the proposed CIP Reliability Standard and the associated Implementation Plans

Exhibit F — Table of CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby requests the Federal Energy Regulatory Commission ("FERC") to approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of FERC's regulations, 18 C.F.R. §39.5 the following proposed Reliability Standards:

- CIP-002-4 – Cyber Security — Critical Cyber Asset Identification (CIP-002-4)
- CIP-003-4 – Cyber Security — Security Management Controls (CIP-003-4)
- CIP-004-4 – Cyber Security — Personnel & Training (CIP-004-4)
- CIP-005-4 – Cyber Security — Electronic Security Perimeter(s) (CIP-005-4)
- CIP-006-4 – Cyber Security — Physical Security of Critical Cyber Assets (CIP-006-4)
- CIP-007-4 – Cyber Security — Systems Security Management (CIP-007-4)
- CIP-008-4 – Cyber Security — Incident Reporting and Response Planning (CIP-008-4)
- CIP-009-4 – Cyber Security — Recovery Plans for Critical Cyber Assets (CIP-009-4)

The NERC Board of Trustees approved the proposed Reliability Standards on January 24, 2011 and recommended they be added to the NERC Reliability Standards. In this filing, NERC requests FERC approval of the proposed Reliability Standards and the associated implementation plans for the CIP Reliability Standards. Additionally, NERC requests that these standards become effective on the first day of the eighth calendar quarter after Commission approval of CIP-002-4 through CIP-009-4.

Exhibit A to this filing sets forth the proposed Reliability Standards. **Exhibit B** contains the Implementation Plan for the CIP Reliability Standards that are being submitted for approval. **Exhibit C** contains the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the CIP Reliability Standards that are being submitted for approval. **Exhibit D** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706, which was the technical team responsible for developing the proposed CIP

[1] NERC has been certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. *See,* 116 FERC ¶ 61,062 (2006) ("ERO Certification Order).
[2] 16 U.S.C. 824o (2010).

Reliability Standards and associated Implementation Plans. **Exhibit E** contains the development record for the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit F** contains a table of CIP Version 4 Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") Proposed for Approval.

NERC is also filing the proposed CIP Reliability Standards and associated documents and requests for approval with applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

Holly A. Hawkins*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

*Persons to be included on FERC's service list are indicated with an asterisk.

III. BACKGROUND

a. Regulatory Framework

By enacting the Energy Policy Act of 2005,[3] Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system, and with the duty of certifying an Electric Reliability Organization (ERO) that would be charged

[3] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005 (codified at 16 U.S.C. § 824o).

with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 states that all users, owners and operators of the bulk power system in the United States will be subject to the FERC-approved Reliability Standards.

The principal purpose of the proposed CIP Reliability Standards is to provide a cyber security framework for the identification and protection of Critical Cyber Assets to support the reliable operation of the Bulk Electric System.

b. Basis for Approval of Proposed Reliability Standard

Section 39.5(a) of FERC's regulations requires the ERO to file with FERC for its approval each Reliability Standard that the ERO proposes to become mandatory and enforceable in the United States, and each modification to an approved Reliability Standard that the ERO proposes to be made effective. FERC has the regulatory responsibility to approve standards that protect the reliability of the bulk power system. In discharging its responsibility to review, approve, and enforce mandatory Reliability Standards, FERC is authorized to approve those proposed Reliability Standards that meet the criteria detailed by Congress:

> *The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest.*[4]

When evaluating proposed Reliability Standards, FERC is required by statute to give "due weight" to the technical expertise of the ERO. Additionally, in Order No. 693, the Commission noted that it would defer to the "technical expertise" of the ERO with respect to the content of a Reliability Standard. The Commission stated:

> Pursuant to Section 215(d)(2) of the FPA and § 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard or to a Regional Entity organized on an Interconnection-wide basis with respect to a proposed Reliability

[4] Section 215(d)(2) of the FPA, 16 U.S.C. § 824o(d)(2) (2000).

Standard or a proposed modification to a Reliability Standard to be applicable within that Interconnection.[5]

Order No. 672 provides guidance on the fifteen factors FERC will consider when determining whether proposed Reliability Standards meet the statutory criteria.[6]

The proposed CIP Reliability Standards serve the important reliability goal of providing a cyber security framework for the identification and protection of Critical Cyber Assets to support the reliable operation of the Bulk Electric System.

The proposed CIP-002-4 Reliability Standard improves reliability by:

- establishing uniform criteria across all Responsible Entities for the identification of Critical Assets,
- establishing a list of Critical Cyber Assets for each Responsible Entity based on its list of Critical Asserts, and
- requiring updates to each list as necessary and an annual review.

Additionally, the proposed CIP Reliability Standards CIP-003-4, CIP-004-4, CIP-005-4, CIP-006-4, CIP-007-4, CIP-008-4, and CIP-009-4 are being submitted for approval with conforming changes to the version numbers, the Applicability section, and the Compliance Enforcement Authority sections.

c. Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC *Standard Processes Manual*,

[5] *Mandatory Reliability Standards for the Bulk-Power System*, 118 FERC ¶ 61,218, FERC Stats. & Regs. ¶ 31,242 (2007) ("Order No. 693") at P 9, *Order on Reh'g, Mandatory Reliability Standards for the Bulk-Power System*, 120 FERC ¶ 61,053 ("Order No. 693-A") (2007).

[6] *See, Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, FERC Stats. & Regs*., ¶ 31,204 at PP 320-338 ("Order No. 672"), *order on reh'g*, FERC Stats. & Regs. ¶ 31,212 (2006) ("Order No. 672-A") at PP 320-338.

which is incorporated into the Rules of Procedure as Appendix 3A. In its ERO Certification Order, FERC found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards.[7]

The Development Process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to FERC.

The work culminating in this filing originated in FERC Order No. 706.[8] FERC Order No. 706 at Paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.[9]

Prior to the development of the proposed CIP Version 4 Reliability Standards, the Standard Drafting Team developed the CIP-002-2 through CIP-009-2 standards to comply with the near-term, specific directives of FERC Order No. 706. That version of the standards was approved by FERC on September 30, 2009 with additional directives to be addressed within 90

[7] Order No. 672 at PP 268, 270.
[8] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶61,040 (January 18, 2008) ("Order No. 706").
[9] *Id*. at P 236.

days of the order.[10] In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 standard, which were approved by FERC in March 2010.[11]

The standard drafting team has continued efforts to address the remaining FERC Order No. 706 directives. The team limited the scope of requirements in the development of CIP-002-4 through CIP-009-4 as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236. The standard drafting team is continuing to address the remaining FERC Order No. 706 directives. The next version of the CIP-002 through CIP-009 Reliability Standards will build on the CIP-002-4 standards' establishment of uniform criteria for the identification of Critical Assets. Given this approach, no Responsible Entity's work toward compliance with the proposed Version 4 CIP Reliability Standards will be wasted. A phased approach to meeting the directives in FERC Order No. 706 has consistently built upon prior versions of the CIP-002 through CIP-009 standards to enhance the reliability of the Bulk Electric System. While the standard drafting team is still working to determine what form the next version of the CIP Reliability Standards will take, with the revisions in Version 4, an established baseline of cyber protection will be extended to all Bulk Electric System Cyber Assets.

The proposed CIP-002-4 through CIP-009-4 Reliability Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. The proposed CIP-002-4 standard requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the

[10] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶61,291 (September 30, 2009) ("September 30, 2009 Order").
[11] *Order on Compliance*, 130 FERC ¶61, 271 (March 31, 2010) ("March 31, 2010 Order").

Bulk Electric System. These Critical Assets are to be identified through the application of the "bright-line" criteria contained in Attachment 1 – Critical Asset Criteria of the CIP-002-4 standard. The remaining CIP Reliability Standards, CIP-003-4 through CIP-009-4, contain conforming changes to match the versioning of CIP-002-4. There are no substantive changes to those standards.

The proposed CIP Reliability Standards set out in **Exhibit A** have been developed and approved by industry stakeholders using NERC's *Reliability Standards Development Procedure* and its replacement, the NERC *Standards Processes Manual*.[12] The proposed CIP Reliability Standards were approved by the NERC Board of Trustees on January 24, 2011.

IV. JUSTIFICATION FOR APPROVAL OF PROPOSED MODIFICATIONS TO RELIABILITY STANDARDS

a. Section Overview

This section summarizes the development of the proposed CIP Reliability Standards. The discussion in this section is also intended to demonstrate that the proposed modifications meet the criteria for approval established by FERC. That is, the proposed modifications to the CIP Reliability Standards ensure that they are just, reasonable, not unduly discriminatory or preferential and in the public interest.[13]

Exhibit A to this filing sets forth the proposed Reliability Standards. **Exhibit B** contains the Implementation Plan for the CIP Reliability Standards that are being submitted for approval.

[12] NERC's *Reliability Standards Development Procedure* is available on NERC's website at http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf. Note that FERC approved the new Reliability *Standard Processes Manual* on September 3, 2010 (FERC Docket No. RR10-12-000), which replaces the *Reliability Standards Development Procedure Version 7* in its entirety. NERC developed this standard in accordance with the *Reliability Standards Development Procedure Version 7* until the *Standard Processes Manual* was approved on September 3, at which time that procedure was used to complete development of the proposed standards.

[13] *See* Order No. 672.

Exhibit C contains the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for the CIP Reliability Standards that are being submitted for approval. **Exhibit D** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706 that was responsible for drafting the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit E** contains the development record for the proposed CIP Reliability Standards and associated Implementation Plans. **Exhibit F** contains a table of CIP Version 4 VRFs and VSLs Proposed for Approval

This extensive development record includes successive drafts of the standard, the ballot pool, the final ballot results by registered ballot body members, and stakeholder comments received during the development of the proposed CIP Reliability Standards, as well as a discussion regarding how those comments were considered in developing them.

The proposed CIP-002-4 Reliability Standard requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1 of CIP-002-4.

The following changes were made to the approved Reliability Standard CIP-002-3 in the development of CIP-002-4:

- The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54;
- Requirement R1, which required Responsible Entities to identify and document a risk-based assessment methodology to identify Critical Assets was modified;

- Requirement R2 was modified to replace the risk-based assessment methodology with a set of uniform criteria for identifying Critical Assets provided in Attachment 1;
- Requirement R3 was modified to provide direction on how to identify shared Cyber Assets at generation plant sites;
- Requirement R4 was modified to remove the reference to risk-based assessment methodology;
- Measure M3 was modified to clarify what records Responsible Entities were required to retain;
- The Compliance section was modified to clarify the Compliance Enforcement Authority under various scenarios; and
- Attachment 1 was added to provide uniform criteria for the identification of Critical Assets.

The remaining CIP Reliability Standards CIP-003-4 through CIP-009-4 contain proposed changes conforming to the CIP-002-4 standard.

The Applicability section in CIP-002-3 was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. The "Rationale and Implementation Reference Document" that was posted during the balloting process,[14] provides guidance for and clarification of Attachment 1 of CIP-002-4. Attachment 1 describes the Critical Asset Criteria a covered entity shall consider in identifying its Critical Assets. This document states on page 6

[14] *See*, http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean_20101220.pdf,

that “these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction.” Additionally, this document provides that “[t]here may be facilities, equipment, or systems which may be in a nuclear facility associated with the Bulk Electric System which are outside of the regulatory realm of these nuclear organizations.” This guidance, in conjunction with the exemption included in Section 4.2.3 of the proposed CIP-002-4 standard, provides that a U.S. nuclear power plant facility that has a verified cyber security plan under 10 C.F.R. Section 73.54 which includes all nuclear power plant systems, structures, and components is exempt from CIP-002-4 requirements, and therefore is not responsible for complying with the CIP-002-4 requirements, including the Critical Asset Identification requirement in Requirement R1 and Attachment 1. If any nuclear power plant systems, structures, and components are not covered under a verified cyber security plan, those systems, structures, and components must be evaluated for CIP-002-4 applicability.

All prior approved versions of CIP-002 included as the first requirement (Requirement R1): “Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.” This Requirement R1 lists certain assets that must be considered when identifying Critical Assets.

In FERC Order No. 706 at Paragraph 253, the Commission stated that: “the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets.” The Commission therefore directed NERC, in its discretion, to: “incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. “ In addition, the Commission provided in Order No. 706 that: “… we direct either the ERO or its designees to provide

reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System."

In response to these directives, NERC developed guidance documents intended to be used to assist entities in developing their risk-based methodology and Critical Asset identification. Over the past two years NERC has conducted various reviews of risk-based methodologies developed by many entities of varying sizes to comply with CIP-002 Requirement R1 and determined that the existing methodologies generally do not adequately identify all Critical Assets. Accordingly, NERC charged the standard drafting team with developing bright line criteria that could be used to identify Critical Assets rather than relying on an entities' existing risk-based methodology. These criteria are provided in Attachment 1 of the proposed CIP-002-4 standard. With these bright line criteria, NERC fulfills the two Order No. 706 directives identified above.

Because Responsible Entities will no longer have a requirement to develop a risk-based assessment methodology, Requirement R2 of the existing CIP-002-3 standard was modified to replace the risk-based assessment methodology for Critical Asset identification with the criteria provided in Attachment 1of CIP-002-4. This requirement now becomes Requirement R1 of the proposed CIP-002-4 standard.

Requirement R3 of the existing CIP-002-3 standard was modified to provide direction on how to identify shared Cyber Assets at generation plant sites. This requirement now becomes Requirement R2 of CIP-002-4.

Criterion 1.1 of Attachment 1exists to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 of the proposed CIP-002-4 standard further stipulates

that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (*i.e.*, the Critical Asset is the group of units that exceeds the specified value). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the transmission system. In specifying a 15-minute qualification, Requirement R2 includes only those Cyber Assets that would have a real-time impact on the reliable operation of the Bulk Electric System.

In a generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This is illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility. In this case, the compromise of the cyber asset may result in an inability of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant amount of time before this affects real-time operation—time during which detection and remediation may be able to be effected.

Requirement R2 and Criterion 1.1 of Attachment 1 both reference a "group of generating units (including nuclear generation) at a single plant location. . . ." This language refers only to generation owners or operators with multiple generators at a single plant location (*e.g.*, gas and nuclear generation at a single site). In the case of nuclear generation, the only Cyber Assets that would be evaluated are those that are not covered under a verified cyber security plan under 10 C.F.R. Section 73.54.

Requirement R4 of CIP-002-3 was modified to remove the reference to risk-based assessment methodology. This requirement now becomes Requirement R3 of CIP-002-4.

Attachment 1 of CIP-002-4 provides uniform criteria for the identification of Critical Assets across all Responsible Entities. A form of these criteria was first proposed in a version of CIP-002-4 that was posted for informal industry comment on December 19, 2009. The standard drafting team analyzed comments from industry and subsequently posted a new document for industry comment—CIP-010-1—on May 4, 2010. The team analyzed these comments from industry and continued to refine the criteria.

NERC then issued a data request to the industry, in accordance with Section 1600 of the NERC Rules of Procedure, in order to gather empirical data that could be used to guide the determination of the final criteria used in the development of the CIP-002-4 standard. Section 1600 of the NERC Rules of Procedure gives NERC the authority to request data or information that is deemed necessary to meet its obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of FERC's regulations. The results of this data request were analyzed and used to develop a new proposed CIP-002-4 standard that was posted for industry comment on October 20, 2010. After two ballot and comment periods, the industry approved the CIP-002-4 standard and the associated Attachment 1.

The following discussion is an analysis of each of the criterion included in Attachment 1, including the applicable responses from the NERC data request. Each criterion is listed, followed by a summary of the NERC data request responses. Each section concludes with a discussion of the justification for each criterion.

Criterion 1.1

1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.1. Nuclear generation Facilities. (17 using CIP-002-3, 88 using this criterion)

1.2. A generating unit or a group of generating units at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding: (59 using CIP-002-3, 229 using this criterion)

a. the Contingency Reserve requirement of the Reserve Sharing Group or of the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed, or

b. the lowest value of the Contingency Reserve requirement of the associated Balancing Authority, for the 12 months preceding the identification or reassessment of the group of generating units, or

c. 2000 MW.

The drafting team, after much debate and evaluation of comments, determined that a Bulk Electric System reliability criterion should not be solely based on fuel type. In addition, the team received feedback that the wording of item 1.2 in the data request was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team therefore performed an informal survey of the Regional Entities and identified what the megawatt value of the reserve sharing would be for various groups. The Regional Entities sourced this criterion partly from the Contingency Reserve requirements in the NERC BAL-002 Reliability Standard, the purpose of which is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, BAL-002 requires that "as a minimum, the Balancing Authority or Reserve Sharing

Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." Additionally, regarding the use of net Real Power capability, the standard drafting team sought to use a value that could be verified through the existing MOD-024 requirements.

The standard drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions. Using this number and data reported by the U.S Energy Information Administration at http://www.eia.doe.gov/cneaf/electricity/page/capacity/existingunits2008.xls, the team determined that approximately 146 generators in the United States would be classified as Critical Assets using this criterion. This accounts for 29% of the installed generator capacity in the United States.

Criterion 1.2

1.2 Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

NERC Data Request (summary results in parenthesis):

1.3. Any reactive resource, including synchronous condensers and static VAR compensators not associated with Generation Facilities, sharing a common Cyber Asset or common Cyber Assets, excluding control centers, that would have an impact on the reliable operation of the group of Facilities within 15 minutes, singularly or in combination, with aggregate rated net Reactive Power capability of 1,000 MVAR or more. (9 using CIP-002-3, 22 using this criterion)

The team received comments that some of the questions in the Data Request were difficult to understand. One of the main reasons this particular criterion caused confusion was

that it defined Critical Assets by using Critical Cyber Assets, which are not evaluated until Requirement R3. After careful consideration, the team determined that Criterion 1.2 in CIP-002-4 captured the same facilities that were captured in Item 1.3 of the NERC Data Request. However, the nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. Therefore, the value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

Criterion 1.3

1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

NERC Data Request (summary results in parenthesis):

1.4 Any generation Facility that the Planning Coordinator identifies as Reliability "must run" assigned units. (14 using CIP-002-3, 44 using this criterion)

The drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid Bulk Electric System Adverse Reliability Impacts in the long term planning horizon are designated as Critical Assets. These Facilities may be designated as "Reliability Must Run," which is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement using terms included in the NERC Glossary. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In

cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation. The standard drafting team does not believe that the changes from the NERC Data Request to criterion 1.3 will result in a significant change to the number of assets indentified as a Critical Asset.

Regarding the "long-term planning horizon" criterion, the standard drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons",[15] which defines "long-term planning horizon" as "a planning horizon of one year or longer."

Criterion 1.4

1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan.

NERC Data Request (summary results in parenthesis):

1.5 Any Blackstart Resource contained in the Transmission Operator's restoration plan. (337 using CIP-002-3, 540 using this criterion)

The standard drafting team determined that the change from the NERC Data Request to criterion 1.3 would result in a significant change in the number of assets indentified as a Critical Asset. The EOP-005-2 Reliability Standard requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. Criterion 1.2 designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term "Blackstart Capability Plan" has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

[15] *See*, http://www.nerc.com/files/Time_Horizons.pdf.

In response to concerns received regarding the communication to Bulk Electric System asset owners and operators of their roles in the Restoration Plans, Transmission Operators are required, pursuant to NERC standard EOP-005-2, to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Criterion 1.5

1.5 The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

NERC Data Request (summary results in parenthesis):

1.9. The Facilities comprising Cranking Paths contained in a Transmission Operator's restoration plan. (981 using CIP-002-3, 1598 using this criterion)

The drafting team received many questions concerning what was intended to be captured in the data request. Commenters pointed out that many options exist for Cranking Paths, and many Transmission Operators develop extensive restoration plans that include multiple Cranking Paths in order to provide flexibility to System Operators in actual restoration scenarios. This may lead to most, if not all, of their Bulk Electric System assets being declared Critical Assets, which could therefore lead to the undesirable result of eliminating those options in restoration plans going forward. Based on these comments, the standard drafting team determined that the most critical elements in the Cranking Path are the points at which no options exist for the System Operator. While it cannot be determined with certainty how the change will affect the

final Critical Asset numbers, the standard drafting team believes that at a minimum, currently declared Critical Assets using existing risk based methodologies will remain on future Critical Asset lists. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

Criterion 1.6

1.6 Transmission Facilities operated at 500 kV or higher.

NERC Data Request (summary results in parenthesis):

1.6. Transmission Facilities operated at 500kV or higher. (270 using CIP-002-3, 436 using this criterion)

There was no change from what was included in the Data Request to criterion 1.6. Therefore there is no expected change to the numbers reported. While the standard drafting team believes that Facilities operated at 500 kV or higher did not require any further qualification for their role as Critical Assets to the interconnected Bulk Electric System, Facilities in the lower Extra High Voltage ("EHV") range should have additional qualifying criteria for inclusion as a Critical Asset.

It should be noted that if the collector bus for a non-Critical Asset generation plant (*i.e.*, the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." Therefore, this collector bus would not be a Critical Asset because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

Criterion 1.7

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

NERC Data Request (summary results in parenthesis):

1.7. Transmission Facilities with four or more Transmission lines operated at 300 kV or higher in the Eastern Interconnection or the Western Interconnection. (140 using CIP-002-3, 224 using this criterion)

1.8. Transmission Facilities with four or more Transmission lines operated at 200 kV or higher in the Texas Interconnection or the Quebec Interconnection. (48 using CIP-002-3, 115 using this criterion)

The threshold for the criterion was lowered from four to three in the Eastern and Western Interconnection, and raised from 200 kV to 300kV in the Texas Interconnection and the Quebec Interconnection. Based on the survey results, the standard drafting team believes that more Facilities will be captured under criterion 1.7 than the criterion included in the Data Request. Criterion 1.7 includes the lower end of the EHV range for Transmission Facilities between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have a significant impact on the Bulk Electric System. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the standard drafting team also included additional qualifications that would ensure the required level of impact to the Bulk Electric System. At the lower end of the EHV spectrum, the drafting team excluded radial facilities that would only

provide support for single generation facilities and specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

Criterion 1.8

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

NERC Data Request (summary results in parenthesis):

1.10 Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). (115 using CIP-002-3, 151 using this criterion)

Commenters stated that Item 1.10 in the data request was confusing for entities to determine the applicability if this item, because a change in operation of a Transmission Facility does not violate an IROL. The standard drafting team revisited the intent behind the criterion, which was to include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2—Establish and Communicate System Operating Limits, Requirements R5.1.1 and R5.1.3. The criterion was changed to reflect this, and the standard drafting team now believes that more Facilities will be captured with the revised criterion than the criterion included in the Data Response.

Criterion 1.9

1.9 Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

NERC Data Request (summary results in parenthesis):

1.11. Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). (0 using CIP-002-3, 0 using this criterion)

Commenters noted that Item 1.11 in the data request was confusing for entities to determine the applicability if this Item because a change in operation of a Transmission Facility does not violate an IROL. The team revisited the intent behind the criterion and FAC-014.2, which is to include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2—Establish and Communicate System Operating Limits, Requirements R5.1.1 and R5.1.3. The wording of criterion 1.9 was changed to reflect this intent. The standard drafting team believes that as the impacts of FACTS devices become more prevalent on the Bulk Electric System, more Facilities will be captured with the revised criterion than the Data Request.

Criterion 1.10

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

NERC Data Request (summary results in parenthesis):

1.12. Transmission Facilities providing the generation interconnection that if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criterion 1.1. (39 using CIP-002-3, 82 using this criterion)

Criterion 1.10 designates those Transmission Facilities as Critical Assets that provide the generation interconnection for generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. The criterion was changed to add Transmission Facilities providing the generation interconnection for Blackstart Resources. Although the majority of these facilities will likely be captured in criterion 1.5 (Cranking Path), this criterion was added to ensure that all Transmission Facilities providing the generation interconnection for generation Critical Assets be designated as Critical Assets.

Criterion 1.11

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

NERC Data Request (summary results in parenthesis):

1.13. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities (46 using CIP-002-3, 123 using this criterion)

There were no significant changes from the data request to Criterion 1.11, therefore there is no expected impact to the numbers reported in response to the data request. Criterion 1.11 is based on NUC-001-2 R9.2.2—Identification of facilities, components, and configuration restrictions that are essential for meeting the [Nuclear Plant Interface Requirements] NPIRs."

NUC-001-2 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, Requirement R9.3.6 requires "Coordination of physical and cyber security protection of the Bulk Electric System at the nuclear plant interface to ensure each asset is covered under at least one entity's plan."

Criterion 1.12

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

NERC Data Request (summary results in parenthesis):

1.14. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have impact beyond the local area. (105 using CIP-002-3, 158 using this criterion)

Commenters expressed concern that the phrase "impact beyond the local area" might be interpreted many different ways. After careful consideration, the standard drafting team chose to designate as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure Bulk Electric System operation within IROLs. The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed because IROL is defined as "A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." By using

the definition of IROL, the loss or compromise of any of these Critical Assets would have Wide Area impacts, meeting the original intent of the NERC Data Request. While it cannot be determined with certainty how the change will affect the final numbers, the standard drafting team believes that, at a minimum, currently declared Critical Assets using existing risk based methodology will remain on future Critical Asset lists.

Criterion 1.13

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

NERC Data Request (summary results in parenthesis):

1.15. Common control system(s) critical to automatic load shedding that are capable of shedding 300 MW or more. (12 using CIP-002-3, 13 using this criterion)

This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding ("UFLS") and Under Voltage Load Shedding ("UVLS") schemes. Some commenters noted that including this criteria might inadvertently require all SCADA systems with the capability of shedding load to be declared as Critical Assets, even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of this criterion. Other commenters stated that this item needed to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Additionally, the criterion needed to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just systems that are "capable" of load shedding.

In light of the comments received, the drafting team chose to change the criterion to specifically include only those systems that did not require human operator initiation, and targeted in particular those UFLS facilities and systems and UVLS facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of load shedding 300 MW or more. While these qualifying systems require a human operator to arm the system, once armed, they trigger automatically. Therefore the criteria to designate these systems as Critical Assets removed the human operator initiation requirement from criterion 1.13. Additionally, the 300MW threshold is consistent with prior versions of CIP-002. The standard drafting team does not believe that the change will reduce the number of systems classified as Critical Assets below the number reported in response to the NERC Data Request.

Criterion 1.14

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

NERC Data Request (summary results in parenthesis):

1.16. Any primary control center or any backup control center used to perform Reliability Coordinator functions. (44 using CIP-002-3, 38 using this criterion)

There were no changes to the criteria from the NERC Data Request to Criterion 1.14, therefore there is no expected impact to the numbers reported. A follow up to a few respondents served to clarify why the number went down. There was confusion about how to classify a control center that performs multiple functions. After further discussion with the entities, it was clear that the net number for all control centers would be a more accurate count of Critical Assets. The standard drafting team believes that the sum of Critical Assets declared under the

new criteria 1.14, 1.15, 1.16, and 1.17 will total more than the sum of the responses from the NERC Data Request items 1.16, 1.17, 1.18, 1.19.

Criterion 1.15

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.16. Any control center or systems or any backup control center or systems used to perform Generator Operator functions for generation that has an aggregate highest rated net Real Power capability in the preceding 12 months exceeding:

a. the lowest value of the Contingency Reserve requirement of the associated Balancing Authority, for the 12 months preceding the identification or reassessment of the generating unit, or

b. 2000 MW, if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established. (81 using CIP-002-3, 121 using this criterion)

The analysis used to develop criterion 1.15 is similar to the development of criterion 1.1. In addition, the drafting team believed that any generation control center that controls generation that is designated a Critical Asset must also be classified as a Critical Asset. For this reason, criteria 1.3 and 1.4 were added to the proposed CIP-002-4 standard. The standard drafting team believes that adding the additional criteria and lowering the MW threshold to 1500 MW will

increase the number of systems classified as Critical Assets above the number reported in the NERC Data Survey.

Criterion 1.16

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

NERC Data Request (summary results in parenthesis):

1.18. Any primary or backup control center performing Transmission Operator functions performed by primary or backup control centers that remotely control two or more Transmission substations or switching stations operated at 300 kV or above in the Eastern Interconnection or the Western Interconnection or 200kV or above in the Texas Interconnection or the Quebec Interconnection, or functionality that remotely controls a Critical Cyber Asset with a High Impact Rating. (195 using CIP-002-3, 221 using this criterion)

Criterion 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12 is to be designated as a Critical Asset due to their direct impact on the operation of identified Critical Assets. In many cases, some Transmission Operator functions are delegated to Transmission Owner control centers. In such cases, these must also be designated as Critical Assets. The drafting team intended for the word "control" to have the same meaning as that found in "Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1" document,[16] which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction." The standard

[16] *See*, http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf.

drafting team believes that most, if not all, of the control centers reported in the NERC Data Survey will still qualify under the approved criterion.

Criterion 1.17

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

NERC Data Request (summary results in parenthesis):

1.17. Any primary or backup control center performing Balancing Authority functions performed by primary or backup control centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 4,000 MW or more in the Eastern Interconnection or the Western Interconnections or 2,000 MW or more in the Texas Interconnection or the Quebec Interconnection. (105 using CIP-002-3, 113 using this criterion)

The analysis used to develop criterion 1.17 is similar to the development of criterion 1.1. In addition, the standard drafting team believes that any generation Balancing Authority control center that controls generation that is designated a Critical Asset must also be classified as a Critical Asset. For this reason, criteria 1.3, 1.4, and 1.13 were added to Criterion 1.17. The standard drafting team believes that adding the additional criteria and lowering the MW threshold to 1500 MW will increase the number of systems classified as Critical Assets above the number reported in response to the NERC Data Request.

The following Item was included in the NERC Data Request but was not included as a criterion in CIP-002-4:

1.20. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include.

This item was included in the NERC Data Request to determine whether and what additional items on existing Critical Asset lists may not meet the new criteria included in Attachment 1. There were several entities that were contacted that had a significant number of entries in this category. The overwhelming response received was that these assets were placed on the Critical Asset list for reasons other than Bulk Electric System reliability. For example, some entities placed large industrial loads or other retail loads that have little impact to Bulk Electric System reliability. Others included every generator they owned, regardless of size, in their Critical Asset methodologies. In no case did the standard drafting team determine that the assets that were included in the responses to this Data Request question could also be assets that impacted Bulk Electric System reliability.

In summary, NERC believes that the application of the uniform criteria included in the proposed Attachment 1 to the CIP-002-4 Reliability Standard will result in more Bulk Electric System assets being declared as Critical Assets, as demonstrated in the analysis of each criterion included Attachment 1. This, in turn, will result in the inclusion of more Bulk Electric System assets as Critical Cyber Assets. While some entities may have a few assets taken off of its existing Critical Asset list under the criteria proposed in CIP-002-4, it is expected that, overall, more Bulk Electric System assets in North America will be classified as Critical Assets. Additionally, it is anticipated that the application of the uniform criteria in Attachment 1 will result in a more consistent identification of Critical Assets by all Responsible Entities.

The proposed CIP-002-4 Reliability Standard contains three requirements summarized as follows:

Requirement R1 mandates that each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

Requirement R2 mandates that each Responsible Entity shall develop a list of Critical Cyber Assets associated with the list of Critical Assets developed in Requirement R1. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of the CIP-002-4 standard, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Requirement R3 mandates that a senior manager or delegate for each Responsible Entity shall approve annually the list of Critical Assets and the list of Critical Cyber Assets, even if that list contains no elements.

b. Demonstration that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest

In order to approve a Reliability Standard proposed by the ERO, FERC must determine, after notice and opportunity for public hearing, that the standard is just, reasonable, not unduly discriminatory or preferential and in the public interest.[17] In Order No. 672, FERC identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Consideration of how the proposed CIP Reliability Standards meet the guidelines identified by FERC in Order No. 672 as necessary to concluding a Reliability Standard meets the statutory criteria follows:

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal

Order No. 672 at P 321. *The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cyber security protection.*

The proposed CIP Reliability Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to

[17] Section 215(d)(2)(A) of the FPA; 18 C.F.R. §39.5.

these Cyber Assets. Proposed Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

2. Proposed Reliability Standards must contain a technically sound method to achieve the goal

Order No. 672 at P 324. *The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.*

The proposed CIP Reliability Standards achieve their stated goal of providing a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. Specifically, the proposed Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria included in Attachment 1 of the proposed CIP-002-4 standard.

Requirement R1 mandates that each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. This will ensure that each Responsible Entity evaluates its entire portfolio of Bulk Electric System assets against the criteria in Attachment 1 to determine those assets that are critical to the reliable operation of the Bulk Electric System.

Requirement R2 mandates that each Responsible Entity shall develop a list of Critical Cyber Assets associated with its list of Critical Assets developed in response to Requirement R1.

This will ensure that each Responsible Entity examines each Critical Asset to find any Cyber Asset that could impact the real time operation of the Critical Asset.

Requirement R3 mandates that a senior manager or delegate for each Responsible Entity shall approve annually the list of Critical Assets and the list of Critical Cyber Assets, even if that list contains no elements. This will ensure that the senior management for each Responsible Entity has verified that Requirements R1 and R2 have been properly performed and validated.

The rest of the CIP Reliability Standards mandate the minimum protection that must be provided to Critical Cyber Assets. Reliability Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Reliability Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Reliability Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Reliability Standard CIP-006-4 ensures the implementation of a physical security program for the protection of Critical Cyber Assets. Reliability Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Reliability Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Reliability Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

The proposed CIP Reliability Standards have been developed by a standard drafting team with a broad base of Bulk Electric System and cyber security knowledge following the scope identified in the Standard Authorization Request that resulted in the initiation of NERC Project 2008-06 Cyber Security Order 706. The standard drafting team for this project adhered to NERC's regulatory-approved standards development process, which allows for industry comment and ballot of the proposed standards. Extensive industry comments on the proposed standards were received and evaluated through several postings. Many of the comments have been incorporated into the final draft of the standards, resulting in refined, high quality standards.

3. Proposed Reliability Standards must be applicable to users, owners, and operators of the bulk power system, and not others

Order No. 672 at P 322. *The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.*

The proposed CIP Reliability Standards are applicable only to Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Service Providers, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, Load Serving Entities, NERC, and Regional Entities. These entities are users, owners, or operators of the bulk power system,

4. Proposed Reliability Standards must be clear and unambiguous as to what is required and who is required to comply

Order No. 672 at P 325. *The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.*

Each of the requirements in the proposed CIP-002-4 Reliability Standard is clear in identifying the required performance (what) and the responsible entity (who):

Requirement R1 - Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the

criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall update this list as necessary, and review it at least annually.

Requirement R2 - Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Requirement R3 - Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

The remaining proposed CIP Reliability Standards, CIP-003-4 to CIP-009-4, retain the same requirement language as the previous FERC approved standards and have already been determined to meet this criterion.

5. Proposed Reliability Standards must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation

Order No. 672 at P 326. *The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.*

Each primary requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines. The table included in **Exhibit F** shows the VRFs and VSLs resulting in the indicated range of penalties for violations.

6. Proposed Reliability Standards must identify clear and objective criterion or measures for compliance, so that it can be enforced in a consistent and non-preferential manner

Order No. 672 at P 327. *There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.*

The proposed CIP Reliability Standards identifies clear and objective criteria in the language of the requirements so that that the standards can be enforced in a consistent and non-preferential manner. The language in the requirements is unambiguous with respect to the applicable entity expectations. Each requirement has a single associated measure.

7. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently, but do not necessarily have to reflect "best practices" without regard to implementation cost

Order No. 672 at P 328. *The proposed Reliability Standard does not necessarily have to reflect the optimal method, or "best practice," for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.*

The proposed CIP Reliability Standards helps the industry achieve the stated goals of identifying Critical Assets and Critical Cyber Assets to ensure Bulk Electric System reliability effectively and efficiently. While there may be an increase in implementation costs as the number of Critical Assets increase under the methodology in proposed CIP-002-4, the NERC Board of Trustees and the industry approved the revised methodology because there is recognition that it is needed to help ensure bulk power system reliability. Accordingly, the costs associated with implementing the proposed CIP-002-4 through CIP-009-4 Reliability Standards are not determined to be excessive or unreasonably burdensome.

8. Proposed Reliability Standards cannot be "lowest common denominator," i.e., cannot reflect a compromise that does not adequately protect bulk power system reliability

Order No. 672 at P 330. *A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a "lowest common denominator" Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.*

The proposed CIP Reliability Standards do not aim at "lowest common denominator." The proposed CIP-002-4 standard provides clear and uniform criteria for identifying Critical Assets on the Bulk Electric System. The remaining proposed CIP Reliability Standards, CIP-003-4 to CIP-009-4, retain the same requirement language as the previous FERC approved standards and have already been determined to meet this criterion.

9. ***Proposed Reliability Standards may consider costs to implement for smaller entities but not at consequence of less than excellence in operating system reliability***

Order No. 672 at P 330. *A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a "lowest common denominator" Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.*

The proposed CIP Reliability Standards do not create any differentiation in requirements based on size. All entities, small and large, are expected to comply with these standards in the same manner.

10. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one area or approach

Order No. 672 at P 331. *A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.*

The requirements in the proposed CIP Reliability Standards apply throughout North America, with no exceptions. The proposed CIP Reliability Standards are a set of standards that will be universally applicable in the portions of the United States and Canada that recognize NERC as the ERO.

11. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid

Order No. 672 at P 332. *As directed by section 215 of the FPA, the Commission itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.*

The proposed CIP Reliability Standards enhance the operation and reliability of the grid and do not constrain competition or restrict transmission capability. The purpose of the proposed CIP Reliability Standards is to provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

Specifically, Reliability Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. Proposed CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. CIP-005-4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. CIP-006-4 ensures the implementation of a physical security program for the protection of Critical Cyber Assets. CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

The proposed CIP Reliability Standards do not have a business practice impact and thus will not result in a negative effect on competition.

12. The implementation time for the proposed Reliability Standards must be reasonable

Order No. 672 at P 333. *In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.*

The Implementation Plan (attached as **Exhibit B**) and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (attached as **Exhibit C**) are reasonable. The Implementation Plan provided in **Exhibit B** specifies how Responsible Entities should transition during the timeframe from FERC acceptance of the proposed CIP Version 4 standards until the Effective Date of the proposed standards. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities included in **Exhibit C** specifies how Responsible Entities should handle newly identified Critical Cyber Assets and newly Registered Entities following the Effective Date of the proposed CIP Reliability Standards.

Based on precedent and lessons learned from past practice, NERC believes the length of time between FERC approval of the proposed CIP Version 4 standards and the effective date is reasonable. This implementation plan time period is consistent with the implementation plan approved by FERC for Version 1 of the CIP Reliability Standards and the implementation plan approved for Registered Entities identifying their first Critical Cyber Asset. Additionally, it takes time to perform a thorough examination of all Bulk Electric System assets to determine whether they meet the criteria included in Attachment 1. Furthermore, additional time must be spent evaluating each Critical Asset to determine all Critical Cyber Assets. In addition, new equipment may have to be installed by Responsible Entities in order to meet the requirements of the CIP-003-4 through CIP-009-4 Reliability Standards.

The following scenarios are provided to further clarify potential implementation issues:

Scenario 1: A newly registered entity that is subject to the CIP Reliability Standards or an existing Responsible Entity identifies a new Critical Cyber Asset prior to FERC acceptance of these proposed CIP Reliability Standards. Under this scenario the entity is subject to the requirements in CIP-002-4 to CIP-009-4

and shall use the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 3.[18]

Scenario 2: Upon FERC acceptance of these proposed CIP Reliability Standards, a Responsible Entity has existing Critical Cyber Assets and has additional assets that now meet the uniform criteria in Attachment 1 of CIP-002-4 that were not previously identified using its established risk-based identification methodology. Under this scenario the Responsible Entity shall use the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Since these Critical Cyber Assets were not identified using CIP-002-3, the Version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities does not apply. Hence, the Responsible Entity shall be compliant with CIP-002-4 through CIP-009-4 for those previously existing Critical Cyber Assets as well as those additional assets captured by the uniform criteria in Attachment 1 of CIP-004 on the Effective Date of these propose CIP Reliability Standards.

Scenario 3: Upon FERC acceptance of these proposed CIP Reliability Standards, a Responsible Entity has no existing Critical Cyber Assets and has assets that now meet the uniform criteria in Attachment 1 of CIP-002-4 that were not previously identified using its established risk-based identification methodology. Under this scenario, similar to Scenario 2, the Responsible Entity shall use the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of: (i) the Effective Date specified in the Standard, or (ii) the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities. Again, since these assets were only identified using CIP-002-4 and not CIP-002-3, the Version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is not applicable, so the Responsible Entity shall be compliant on the Effective Date of these proposed CIP Reliability Standards.

Scenario 4: After the Effective Date of these proposed CIP Reliability Standards, an entity is newly registered as a Registered Entity that is subject to the CIP Reliability Standards or an existing Responsible Entity identifies a new Critical Cyber Asset. Under this scenario the entity is subject to the requirements in CIP-002-4 to CIP-009-4 and shall use the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 4.

---

[18] *See,* http://www.nerc.com/docs/standards/sar/Imp-Plan_Newly_Identified_CCA_RE_clean_last_approval_2009Nov19.pdf.

Scenario 5: A Responsible Entity that has existing Critical Cyber Assets installs a new Critical Cyber Asset. All new installations of Critical Cyber Assets are required to be compliant upon commissioning, whether under CIP-002-3 to CIP-009-3 or CIP-002-4 to CIP-009-4.

Scenario 6: A Responsible Entity commissions a new planned Bulk Electric System asset 1 month prior to the Effective Date of Version 4. This asset was not determined to be a Critical Asset according to the Entity's Version 3 established risk-based identification methodology, but does meet the uniform criteria in Attachment 1 of CIP-002-4. Under this scenario, the Responsible Entity should be able to determine that the asset will meet the uniform criteria during its planning phase and therefore must be compliant with CIP-002-4 through CIP-009-4 on the Effective Date of these proposed CIP Reliability Standards.

Scenario 7: Prior to the Effective Date of these proposed CIP Reliability Standards, a Responsible Entity that previously had no existing Critical Cyber Assets identifies a new Critical Cyber Asset based upon its existing CIP-002-3 processes and procedures. In addition, this Critical Cyber Asset is associated with a Critical Asset that also meets the uniform criteria in Attachment 1 of CIP-002-4. Under this scenario, the Responsible Entity shall initially determine its Version 3 compliance milestones using the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for Version 3. However, the Responsible Entity may find, if the Critical Cyber Asset was identified after FERC acceptance of these proposed CIP Reliability Standards, that its Version 3 compliance milestones are later than the Effective Date of Version 4, at which point the Version 3 CIP Reliability Standards are already retired. In such a scenario, the Responsible Entity shall use part (ii) of the Implementation Plan in Exhibit B, which specifies that Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on...the compliance milestones specified in Version 3 of the Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities. This phrase in the Version 4 Implementation Plan was included specifically to ensure that the Effective Date of these proposed CIP Reliability Standards does not override a Responsible Entity's previously established compliance milestone schedule.

13. The Reliability Standard development process must be open and fair

Order No. 672 at P 334. *Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's Reliability Standard*

development process if it is conducted in good faith in accordance with the procedures approved by the Commission.

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure, the NERC *Reliability Standards Development Procedure*, and its replacement NERC *Standards Processes Manual*, which is incorporated into the Rules of Procedure as Appendix 3A. In its ERO Certification Order, FERC determined that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the bulk power system. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to FERC. The drafting team developed this standard by following NERC's regulatory-approved standards development process.

14. Proposed Reliability Standards must balance with other vital public interests

Order No. 672 at P 335. *Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.*

The proposed CIP Reliability Standards do not conflict with any vital public interests. Compliance with these proposed CIP Reliability Standards support preventing instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the interconnection.

15. Proposed Reliability Standard must not conflict with prior FERC Rules or Orders.

Order No. 672 at P.444. *a potential conflict between a Reliability Standard under development and a Transmission Organization function, rule, order, tariff, rate schedule, or agreement accepted, approved, or ordered by the Commission should be identified and addressed during the ERO's Reliability Standard Development Process.*

The proposed CIP Reliability Standards do not conflict with any other prior FERC Rules or Orders. The proposed CIP Reliability Standards addresses some of the directives identified in FERC Order No. 706 that were not addressed in prior versions. The standard drafting team is continuing to develop CIP Reliability Standards that meet the rest of the directives identified in FERC Order No. 706.

16. Proposed Reliability Standards must consider any other relevant factors

Order No. 672 at P 323. *In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.*

Order No. 672 at P 337. *In applying the legal standard to review of a proposed Reliability Standard, the Commission will consider the general factors above. The ERO should explain in its application for approval of a proposed Reliability Standard how well the proposal meets these factors and explain how the Reliability Standard balances conflicting factors, if any. The Commission may consider any other factors it deems appropriate for determining if the proposed Reliability Standard is just and reasonable, not unduly discriminatory or preferential, and in the public interest. The ERO applicant may, if it chooses, propose other such general factors in its ERO application and may propose additional specific factors for consideration with a particular proposed Reliability Standard.*

No other factors for FERC's consideration were identified in the development of the proposed CIP Reliability Standards.

c. Violation Risk Factor and Violation Severity Level Assignments

NERC is proposing VRFs and VSLs for CIP Version 4 in this filing consistent with those proposed for CIP Version 3. On December 18, 2009, NERC submitted a petition for approval of CIP Version 2 VRFs and VSLs, which were carried over, in part, from the FERC-approved CIP Version 1 VRFs and VSLs.[19] On December 29, 2009, NERC submitted a petition for approval of CIP Version 3 VRFs and VSLs, which were carried over, in part, from the CIP Version 2

[19] *See*, Petition of the North American Electric Reliability Corporation for Approval of Violation Severity Levels to Critical Infrastructure Protection (CIP) Version 2 Reliability Standards CIP-002-2 through CIP-009-2 and Violation Risk Factors for CIP-003-2 and CIP-006-2, filed in FERC Docket Nos. RM06-22-000 and RD09-7-000 (December 18, 2009).

VRFs and VSLs.[20] FERC issued an Order on January 20, 2011 approving the CIP Version 2 and Version 3 VRFs and VSLs, and directed that a compliance filing be made within 60 days (by March 21, 2011) that modifies certain of the CIP Version 2 and Version 3 VRFs and VSLs in response to the Commission's concerns.[21]

In this filing, NERC is proposing to carry over the CIP Version 4 VRFs and VSLs from CIP Version 3. However, given that the CIP Version 4 standards were developed with proposed VSLs and VRFs prior to the Commission's issuance of the January 20, 2011 Order, NERC recognizes that the proposed CIP Version 4 VRFs and VSLs included in **Appendix F** of this filing do not respond to the Commission's concerns articulated in the January 20, 2011 Order. Accordingly, NERC is hereby submitting with this filing the proposed CIP Version 4 VRFs and VSLs that were balloted with the proposed CIP Version 4 standards prior to the issuance of the January 20, 2011 Order. NERC will make a compliance filing in response to the January 20, 2011 Order proposing modifications to the CIP Version 2 and Version 3 VRFs and VSLs by March 21, 2011. In that filing, NERC will include an updated table of proposed VRFs and VSLs for CIP Version 4, carried over from those proposed for CIP Versions 2 and 3 VRFs and VSLs in compliance with Commission directives, and will request that those VRFs and VSLs be applied to the pending CIP Version 4 standards, as applicable.

[20] *See*, Compliance Filing of the North American Electric Reliability Corporation in Response to the Federal Energy Regulatory Commission's September 30, 2009 Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing, filed in FERC Docket No. RD09-7-000 (December 29, 2009).

[21] *Order on Version 2 and Version 3 Violation Risk Factors and Violation Severity Levels for Critical Infrastructure Protection Reliability Standards*, 134 FERC ¶61,045 (January 20, 2011).

V. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

a. Development History

FERC Order No. 706 at Paragraph 236 directed NERC to develop modifications to the CIP-002-1 Cyber Security – Critical Cyber Asset Identification Reliability Standard to address concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A standards drafting team was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The standard drafting team has been charged with reviewing each of the CIP Reliability Standards to address the modifications identified in FERC Order No. 706. The standard drafting team began meeting in October 2008.

Prior to this filing, the standard drafting team developed the CIP-002-2 through CIP-009-2 Reliability Standards to comply with the near-term specific directives of FERC Order No. 706. The CIP Version 2 standards were approved by FERC in the September 30, 2009 Order with additional directives to be addressed within 90 days of the order. In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 Reliability Standards, which were approved by FERC in the March 31, 2010 Order.

Throughout this period, the standard drafting team has continued its efforts to develop an approach to address the remaining FERC Order No. 706 directives. Most recently, the proposed CIP-010 and CIP-011standards were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the standard drafting team determined it

was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the standard drafting team limited the scope of requirements in this Version 4 of CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in Paragraph 236 of Order No. 706. The plan to address the remaining FERC Order No. 706 directives continues to be developed.

On September 20, 2010, the standard drafting team posted the proposed CIP-002-4 standard for a formal 45-day comment period. During the comment period, the team received 101 sets of comments, including comments from more than 200 different people from approximately 125 companies representing 9 of the 10 Industry Segments. Concurrent with the comment period, a ballot pool was assembled and the first formal ballot was conducted. In the initial ballot, a quorum was achieved, and the weighted sector vote was 43.33% affirmative.

Based on the comments received, a few changes were made to the CIP-002-4 standard. The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. In addition, the effective date was changed to eight quarters after regulatory approval, so that entities are not required to develop and maintain two sets of approved Critical Asset lists and Critical Cyber Asset lists concurrently. Requirements R1 and R2 were modified slightly to clarify that each list must be updated on an ongoing basis, but the review and approval need only occur annually. Conforming changes were made to the compliance section. Significant changes were also made to Attachment 1 to ten of the criteria. The criterion allowing entities to place items on the Critical Asset list at their discretion was deleted. The criterion for control centers was split into three criteria to allow for differentiation

in size for Balancing Authorities and Transmission Operators. All of these changes were made in response to comments received.

In November of 2010, the Standards Committee Executive Committee authorized the standard drafting team to conduct an abbreviated comment period in parallel with a successive ballot, to support providing stakeholders with the opportunity to provide comment, while also supporting the goal of completing this set of revisions to CIP-002 before the end of December 2010. A successive ballot of the proposed CIP Version 4 Reliability Standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Following this ballot, the Project 2008-06 drafting team made minor changes to the CIP-002-4 standard and the associated guidance document and implementation plan. A recirculation ballot was conducted from December 20-30, 2010 and achieved a quorum of 90.49% and a weighted segment approval of 80.56%.

The NERC Board of Trustees approved the proposed CIP Reliability Standards on January 24, 2011 and recommended they be added to the set of NERC Reliability Standards.

VI. CONCLUSION

For the reasons stated above, NERC requests that FERC approve the proposed CIP Reliability Standards as set out in **Exhibit A**, the associated Implementation Plans as set out in **Exhibit B** and **Exhibit C**, and the proposed VRFs and VSLs included in **Exhibit F** in accordance with Section 215(d)(1) of the Federal Power Act and Part 39.5 of FERC's regulations. NERC requests that approvals be made effective in accordance with the effective date provisions set forth in the proposed CIP Reliability Standards.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 10th day of February, 2011.

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

Exhibit A

Proposed CIP-002-4 through CIP-009-4 Reliability Standards submitted for approval

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~3~~4

3. Purpose: NERC Standards CIP-002-~~3~~4 through CIP-009-~~3~~4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-~~3~~4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of ~~a risk-based assessment~~the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first

day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. **Requirements**

~~**R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.~~

~~**R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.~~

~~**R1.2.** The risk-based assessment shall consider the following assets:~~

~~**R1.2.1.** Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.~~

~~**R1.2.2.** Transmission substations that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.3.** Generation resources that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.4.** Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.~~

~~**R1.2.5.** Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.~~

~~**R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.7.** Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.~~

~~**R2.**~~**R1.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the ~~risk-based assessment methodology required~~criteria contained in ~~R1.~~*CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary~~.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement ~~R2~~R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.~~ Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange.~~ The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary.~~ .

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-~~3~~4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1~~, R2,~~ and ~~R3~~R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

~~**M1.** The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.~~

~~M2.~~M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement ~~R2~~R1.

~~M3.~~M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement ~~R3~~R2.

~~M4.~~M3. The Responsible Entity shall make available its ~~approval~~ records of ~~annual~~ approvals as specified in Requirement ~~R4~~R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity ~~for Responsible Entities~~shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not ~~perform delegated tasks~~work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~• For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~1.1.2 ERO for Regional Entity.~~

- ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~1.1.3~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~1.2.~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

~~1.2.1~~1.1.2 ~~Not applicable~~Enforcement Authority.

~~1.3.~~1.2. **Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Indent: Left: 1.5", Hanging: 0.25", Outline numbered + Level: 3 + Numbering Style: Bullet + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5", Tab stops: 1.75", List tab + Not at 1.5"

Self-Reporting

Complaints

~~1.4.~~1.3. **Data Retention**

~~1.4.1~~1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

~~1.4.2~~1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.5.~~1.4. **Additional Compliance Information**

~~1.5.1~~1.4.1 None.

2. Violation Severity Levels (~~Developed separately~~To be developed later.)

E. **Regional Variances**

None identified.

Version History

Version	Date	Action	Change Tracking
1	~~01/~~January 16~~/06~~, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2	~~Approved by NERC Board of Trustees 5/6/09~~	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	~~Revised~~
3		~~Changed~~Updated version number from ~~CIP-002~~-2 to ~~CIP-002~~-3~~.~~ ~~Changed all references to CIP Version "2" standards to CIP Version "3" standards.~~ ~~For Violation Severity Levels, changed, "To be developed later" to "Developed separately."~~	~~Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)~~
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	1/24/11	Approved by the NERC Board of Trustees	

Formatted Table

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~3~~4

3. **Purpose:** Standard CIP-003-~~3~~4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. **Applicability:**

   4.1. Within the text of Standard CIP-003-~~3~~4, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-003-~~3~~4:

   4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

   ~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

   ~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets shall only be required to comply ~~with CIP~~with4CIP-003-3 Requirement R2.

5. **Effective Date:** The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font: Bold

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-~~3~~4 through CIP-009-~~3~~4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-~~3~~4 through CIP-009-~~3~~4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-~~3~~4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment.	

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

		Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with4CIP-003-3 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-~~3~~4

3. Purpose: Standard CIP-004-~~3~~4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-004-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound

Formatted: Font color: Black

Formatted: Font color: Black

security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-~~3~~4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-~~3~~4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not Applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".	

		Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4

3. Purpose: Standard CIP-005-4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Revised.

		Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-~~3~~4

3. Purpose: Standard CIP-005-~~3~~ 4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-~~3~~ 4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~ 4 through CIP-009-~~3~~4.

4. Applicability

4.1. Within the text of Standard CIP-005-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-~~3~~4:

4.2.1 Facilities regulated by the ~~U.S. Nuclear Regulatory Commission or the~~ Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

~~4.2.3~~4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-~~3~~4.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-~~3~~4; Standard CIP-004-~~3~~ 4 Requirement R3; Standard CIP-005-~~3~~ 4 Requirements R2 and R3; Standard CIP-006-~~3~~ 4 Requirement R3; Standard CIP-007-~~3~~ 4 Requirements R1 and R3 through R9; Standard CIP-008-~~3~~4; and Standard CIP-009-~~3~~4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-~~3~~ 4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-~~3~~4.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-~~3~~ 4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-~~3~~ 4 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~3~~4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-~~3~~4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-~~3~~ 4 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	Revised.

		Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4

3. Purpose: Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved	Update version number from "3" to "4"	Update to conform to changes to CIP-

	01/24/2011		002-4 (Project 2008-06)

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Appendix 3

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-~~3~~4

3. Purpose: Standard CIP-006-~~3~~4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-006-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.2~~4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall")

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font: Bold, Font color: Auto

border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~3~~4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~3~~4; Standard CIP-004-~~3~~4 Requirement R3; Standard CIP-005-~~3~~4 Requirements R2 and R3; Standard CIP-006-~~3~~4 Requirements R4 and R5; Standard CIP-007-~~3~~4; Standard CIP-008-~~3~~4; and Standard CIP-009-~~3~~4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~3~~4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~3~~4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entities.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the	

		requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

> **R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> **R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.**

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

> **1.4. Additional Compliance Information**
>
> **1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.**

Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Appendix 3

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~3~~4

3. Purpose: Standard CIP-007-~~3~~4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-007-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-~~3~~4, a significant

Formatted: Font color: Black

Formatted: Font color: Black

change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-~~3~~4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-~~3~~4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-~~3~~4 Requirement R5 and Standard CIP-004-~~3~~4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-~~3~~4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-~~3~~4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-~~3~~4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-~~3~~4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.1~~4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.2~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

Formatted: Font: Bold

Formatted: Tab stops: Not at 3"

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

Formatted: Font: Not Bold

Formatted: Font: Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Tab stops: Not at 3"

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform	

Formatted: Tab stops: Not at 3"

		testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Formatted: Tab stops: Not at 3"

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~3~~4

3. Purpose: Standard CIP-009-~~3~~4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

Formatted: Font color: Black

Formatted: Font color: Black

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entities.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

Formatted: Font: Not Bold

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

Exhibit B

Implementation Plan for Version 4 Cyber Security Standards CIP-002-4 through CIP-009-4

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The effective date of EOP-005-2 is the date that Criteria 1.4 and 1.5 will be used to determine Critical Assets for Responsible Entity.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority
• Interchange Authority
• Transmission Service Provider
• Transmission Owner
• Transmission Operator
• Generator Owner
• Generator Operator
• Load Serving Entity
• NERC
• Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities

For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4, (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage, or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Exhibit C

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for CIP Reliability Standards submitted for approval

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by*

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

the Responsible Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

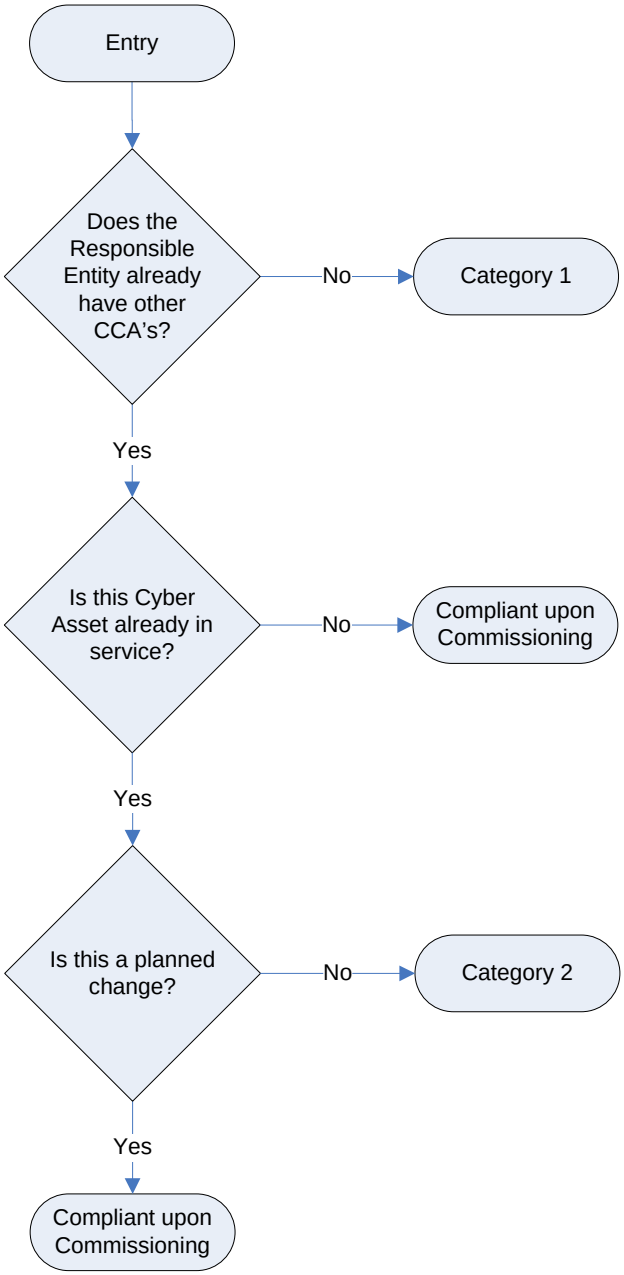


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In

this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the access authorization process.

The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merged plan is being performed. Progress towards meeting milestones and completing the merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly identified Critical Asset, but no newly identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon identification of a Critical Asset without associated Critical Cyber Assets. Only upon identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets[4]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

[4] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5][6] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	**Registration + 12 months**	**Registration + 24 months**
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.
[6] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage.

Exhibit D

Standard Drafting Team Roster for Project 2008-06 Cyber Security
Order 706

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

1. **Chairman**	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
2. **Vice Chairman**	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
3. **Members**	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905) 262-2686 Fx rob.antonishen@ opg.com
4.	Jim Brenton, CISSP-ISSAP Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ercot.com
5.	Jackie Collett Cyber Security Operations Engineer	Manitoba Hydro 1565 Willson Place P.O. Box 815 Winnipeg, Manitoba R3C 2P4	(204) 477-7709 jcollett@hydro.mb.ca
6.	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@ southernco.com
7.	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
8.	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 508-1285 -cell (513) 287-1564 sharon.edwards@ duke-energy.com
9.	Gerald S. Freese Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
10.	William Gross	Nuclear Energy Institute	(202) 739-8123 wrg@nei.org
11.	Jeffrey Hoffman Chief Architect IT Policy & Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm. 380 PO Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 (303) 445-6307 Fx JHoffman@usbr.gov

12.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com
13.	Patricio Leon-Alvarado Engineer, E&TS Compliance and Quality	Southern California Edison One Innovation Way Pomona, CA 91768	(909) 274-1697 (909) 274-1692 Fx Patricio.leon- alvarado@sce.com
14.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
15.	David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue MS: L-MOB-17A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@ entergy.com
16.	David S Revill Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
17.	Scott Rosenberger Director, Security and Compliance	Luminant 1601 Bryan Street 46th Floor Dallas, TX 75201	(214) 812-2412 scott.rosenberger@ energyfutureholdings. com
18.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
19.	Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
20.	Thomas Stevenson Gen Supv Engineering Projects Generation Services Dept	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 - cell Thomas.W.Stevenson @constellation.com
21.	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@ nist.gov
22.	John Van Boxtel CIP Compliance Engineer	Western Electricity Coordinating Council Suite #201 7600 NE 41st Street Vancouver, WA 98662	(360) 713-9090 jvanboxtel@wecc.biz
23.	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com

24.	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
25.	Bradley (Brad) Yeates IT Security Analyst, Principal	Southern Nuclear Operating Company 241 Ralph McGill Blvd. Bin 10030 Atlanta, Ga. 30308	(404) 314-4096 blyeates@southernco .com
Consultant to NERC	Hal Beardall	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Consultant to NERC	Joseph Bucciero President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@ gmail.com
Consultant to NERC	Robert M. Jones Director Florida Conflict Resolution Consortium	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Consultant to NERC	Stuart Langton, PhD Senior Fellow	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@ mindspring.com
NERC Staff	Herb Schrayshuen Vice President and Director of Standards	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx Herb.schrayshuen@ nerc.net
NERC Staff	Howard L. Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx howard.gugel@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@ nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 Fx Scott.Mix@ nerc.net
NERC Staff	David Taylor Director of Standards Development	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@ nerc.net
NERC Staff	Todd Thompson Compliance Investigator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@ nerc.net

Exhibit E

Development Record of the proposed CIP Reliability Standard and the associated Implementation Plans

Project 2008-06
Cyber Security Order 706 Phase II

Activity:
Phase II Reliability Standards

Status:
CIP Version 4 standards (CIP-002-4 through CIP-009-4) were approved by the Board of Trustees on January 24, 2011.

Draft	Action	Dates	Results	Consideration of Comments
CIP-002-4 Clean **(63)** | Redline to last approval **(64)** | Redline to successive ballot **(65)** CIP-003-4 through CIP-009-4 Clean **(60)** | Redline to last approval **(61)** |Redline to last posting **(62)** Implementation Plan Clean **(58)**| Redline to successive ballot **(59)** Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities Clean **(57)**	Recirculation Ballot Vote>>| Info **(66)**	12/20/10-12/30/10	Summary **(68)** Full Record **(67)**	

Supporting Materials: Draft Guidance Document Clean**(55)** | Redline to successive ballot**(56)**				
CIP-002-4 Clean**(46)** | Redline to last approval **(47)**|Redline to last posting**(48)**	Successive Ballot Vote>>>

Draft Guidance Document Clean(37) | Redline to last posting(38) Unofficial Comment Form (Word)(36)				
CIP-002-4 Clean(28) | Redline to last approval (29)(Updated 10/20/10) CIP-008-4 (Updated 10/20/10 Clean(26) | Redline to last approval (27) CIP-003-4, CIP-004-4, CIP-006-4, CIP-007-4, CIP-009-4 Clean (24)| Redline to last approval(25) Implementation Plan for CIP Version 4 Standards(23) Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities clean(21) | Redline to last approval(22) **Supporting Materials:** Comment Form	Initial Ballot Vote>> | Info(32)	10/20/10 - 11/3/10	Summary(34) Full Record (33)	Consideration of comments(35)
	Formal 45-day Comment Period Submit Comments>>| Info(30)	9/20/10 - 11/03/10		Consideration of Comments(31)

(Word)**(20)** Mapping Document**(19)** VRF and VSL Analysis**(18)** Draft Guidance Document**(17)**				
Reliability Standard CIP-010-1 and CIP-011-1 CIP-010-1 **(14)** CIP-011-1 **(13)** **Supporting Materials:** Comment Form (Word) **(12)**	Informal Comment Period Submit Comments>> Info **(15)**	05/04/10 - 06/03/10 (closed)		Consideration of Comments on Question 7 **(16)**
Reliability Standard CIP-002-4 and Guidance Document CIP-002-4 **(7)** Draft Guidance Document **(6)** **Supporting Materials:** Comment Form (Word) **(5)**	Informal Comment Period Submit Comments>> Info **(8)**	12/19/09 - 02/12/10 (closed)	Comments Received **(9)**	Consideration of Comments**(11)** Executive Overview**(10)**
	CIP Standards Revisions Concept Paper Webinar Slides **(4)**	08/25/09		
Cyber Security Concept Paper Categorizing Cyber	Informal Comment Period	07/21/09 - 09/04/09 (closed)	Comments Received **(3)**	

Systems — An Approach Based on BES Reliability Functions **(1)**	Info **(2)** Submit Comments>>			

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

Cyber Security Standards Drafting Team for Project 2008-06

Cyber Security Order 706

to ensure the reliability of the bulk power system

JULY 2009

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

TABLE OF CONTENTS

A. EXECUTIVE SUMMARY 3

B. INTRODUCTION 4

C. BES RELIABILITY FUNCTIONS 9

D. IDENTIFICATION OF BES SUBSYSTEMS 15

E. IMPACT MAPPING OF BES SUBSYSTEMS 16

F. IDENTIFICATION OF BES CYBER SYSTEMS 17

G. CATEGORIZATION OF CYBER SYSTEMS 19

H. FINAL CATEGORIZATION OF CYBER SYSTEMS BASED ON OVERALL IMPACT ON THE BES 21

I. DEFINING THE TARGET OF PROTECTION 23

J. EXTERNAL CYBER SYSTEMS 29

K. APPLYING SECURITY CONTROLS TO THE TARGET OF PROTECTION 30

L. CONCLUSION 31

APPENDIX A: TERMS AND DEFINITIONS 32

Categorizing Cyber Systems:

An Approach Based on Impact on BES Reliability Functions

A. EXECUTIVE SUMMARY

This paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*, proposes a broader and more comprehensive approach for providing appropriate and effective cyber security to protect the systems which support a reliable Bulk Electric System (BES).

The BES is viewed holistically in terms of reliability functions supporting an Adequate Level of Reliability, its supporting BES subsystems and cyber systems, which are categorized based on impact. This process results in a more uniform selection of appropriate security requirements and controls, which reduces risk to the BES caused by a Cyber Security Incident.

The methodology in the approach proposes a mapping of BES subsystems to pre-determined criteria into categories based on their impact on the reliability or operability of the BES. The categorization of BES cyber systems and their elements is based on an analysis of their impact, either directly or indirectly through the BES subsystems, on the BES functions they support. A rigorous analysis of the impact to the BES for any given cyber system results in a deterministically derived categorization of each cyber system.

In defining the cyber systems which constitute the target for protection, this paper considers issues associated with interconnected systems, systems associated with the computing infrastructure supporting these BES cyber systems and systems that are collaterally affected because of their proximity to BES cyber systems.

A crucial undertaking for the drafting team lies in developing these security controls in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry. To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed.

The development of these controls is outside the scope of this paper; the drafting team will seek further industry input in the development phase of the controls framework.

The concepts presented here are a paradigm shift, considering that cyber technology in support of reliability are *systems* intimately associated with the reliability functions that they support.

This paper deals with the identification and classification of BES assets and Cyber Systems. There are a number of other issues raised in FERC Order 706 concerning CIP-002-1 matters that are not addressed in this paper. The SDT will be soliciting industry feedback on those issues as part of the standards development process.

B. INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards aimed at preserving and enhancing the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability or operability** of this system. The overarching mission is preserving and enhancing the reliability of this system, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002 — Cyber Security — Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment." FERC's comments in its Order 706 approving the Cyber Security Standards as well as common perceptions and observations from various other commenters will all be considered as valuable input into this process.

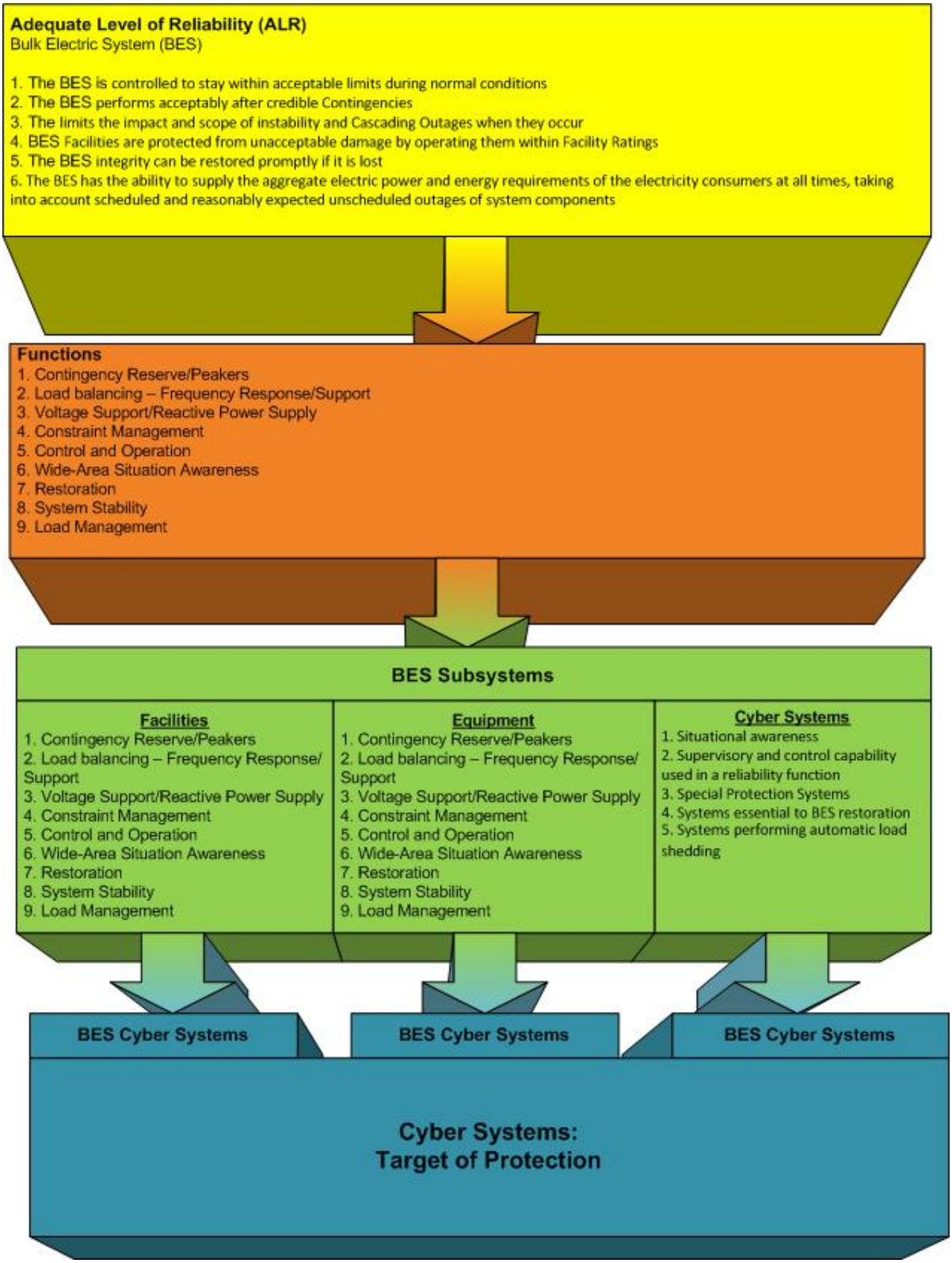
This paper describes an approach based on the concepts of NERC's definition of Adequate Level of Reliability (ALR) and the characteristics of the BES described therein that will achieve this ALR, namely:

1. The Bulk Electric System is controlled to stay within acceptable limits during normal conditions;
2. The Bulk Electric System performs acceptably after credible Contingencies;
3. The Bulk Electric System limits the impact and scope of instability and Cascading Outages when they occur;
4. The Bulk Electric System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The Bulk Electric System's integrity can be restored promptly if it is lost; and
6. The Bulk Electric System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.

This proposed cyber system categorization approach relies on the identification of functions which are essential to achieving these characteristics and the BES subsystems which support these functions. These BES subsystems may be defined as facilities, equipment, or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability.

The methodology proposes to identify all cyber systems which support the reliable operation of the BES; one must note that a cyber system can itself be a BES subsystem if it directly performs one or more of the identified functions and if compromised will impact that function.

Figure 1


Adequate Level of Reliability (ALR)
Bulk Electric System (BES)
1. The BES is controlled to stay within acceptable limits during normal conditions
2. The BES performs acceptably after credible Contingencies
3. The limits the impact and scope of instability and Cascading Outages when they occur
4. BES Facilities are protected from unacceptable damage by operating them within Facility Ratings
5. The BES integrity can be restored promptly if it is lost
6. The BES has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components
Functions
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
BES Subsystems
Facilities
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Equipment
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Cyber Systems
1. Situational awareness
2. Supervisory and control capability used in a reliability function
3. Special Protection Systems
4. Systems essential to BES restoration
5. Systems performing automatic load shedding
BES Cyber Systems
BES Cyber Systems
BES Cyber Systems
Cyber Systems:
Target of Protection

Once BES subsystems and their cyber systems are identified, the methodology requires an analysis based on two major factors:

- A mapping of BES subsystems into categories based on pre-defined criteria which reflect their impact on the reliability or operability of the BES
- A categorization of their associated cyber systems and their elements based on their impact on the functions of the BES subsystems they support.

An analysis of any given cyber system results in a deterministically derived categorization of each cyber system based on its impact on the BES.

The scope of the CIP Cyber Security standards being considered excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies, since they are regulated outside of NERC. Note that there may be facilities, equipment, or systems that may be in a nuclear facility associated with the BES that are outside of the regulatory realm of these nuclear regulatory organizations, and would therefore be regulated under these NERC CIP standards. It is also worth noting that the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliability or operability of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards if they meet the protection requirements of the Cyber Security Standards (for example, if they impact a cyber system that is subject to the standards).

The concepts associated with an impact-based approach to determining the criticality of certain facilities, equipment, and systems are particularly well covered in the Draft Volume 1 of NERC's Security Guideline for the Electric Sector: Identifying Critical Assets. The development of this guidance document was in direct response to a directive by FERC in Order 706. An additional important concept in this approach is the inclusion of assets based on their functions in the operation of the BES. The SDT is currently engaged in an additional guidance document to address the identification of Critical Cyber Assets. The approach proposed by the Cyber Security Standard Drafting Team for the identification and classification of BES subsystems also draws upon the BES functions and asset identification as well as the criteria for Critical Assets sections of the guideline.

The ideas and approaches identified in this concept paper are well-grounded and draw on elements of principles already described in other related, publicly available information, such as the application of a Federal Information Processing Standards 199-like approach to classifying

cyber systems and the National Institute of Standards and Technology's framework for information security risk management, as well as internal SDT discussions on guiding principles used for the development of a cyber systems categorization model and comments and discussions with recognized industry experts from a variety of applicable domains.

The cyber system categorization approach outlined in this concept paper includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact-based methodology to map its BES subsystems into categories based on pre-defined criteria and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact-based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This methodology parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high level objectives, then drilling down into supporting processes.

The relationship of cyber systems to BES reliability is deeper and more inter-related than it might appear on the surface. The readers of this concept paper are encouraged to use all of their experience as they review this paper, but should be prepared to have their assumptions challenged, as this represents a paradigm shift for experienced operating personnel. Consider that cyber technology in support of reliability is not just a piece of hardware or software or a communication circuit, but rather, a *system* intimately associated with the reliability functions that it supports. Cyber systems can have more subtle linkages in addition to the linkage caused by the interconnected bulk electric system.

This concept paper is focused on the identification and classification of BES assets and Cyber Systems. There are a number of other issues raised in FERC Order 706 dealing with CIP-002-1 matters that are not addressed in this paper. The SDT will be soliciting industry feedback on these issues as part of the standards development process.

C. BES RELIABILITY FUNCTIONS

A prerequisite to the start of the identification of BES Subsystems that affect the reliability or the operability of the BES is the identification of functions that support the characteristics of ALR. These functions may contribute to an adequate level of reliability in varying degrees, which would be considered through the impact assessment of the BES subsystem on the reliability or operability of the BES.

The following table provides an illustrative example of the BES Reliability Functions, the BES subsystem mapping criteria, together with sample BES subsystems and cyber systems that could be envisioned. The contents of this table are provided only as possible definitions and are not intended to be a final, comprehensive, and exhaustive list.

Table 1

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Contingency Reserve/Peakers	Single resource or combined resources (sharing a common mode failure) whose output exceeds the Contingency Reserve • Unit capable of starting in 15 minutes or less Transmission facility or facilities, whose loss or compromise may result in the loss of resources identified for contingency reserves (those resources in the above bullet or it could be the loss of an import)	Generating unit(s) whose output exceeds the Contingency Reserve Transmission lines, busses and transformers associated with the such generation	Generation control system Real-time monitoring system used for operation Protective relay Station Automation System AGC Plant control room(s)
Load Balancing Frequency Response/Support	Single resource or combined resources (sharing a common mode failure) whose loss or compromise may result in under-frequency Transmission facility or facilities, whose loss or compromise may result in under-frequency	Generating Unit(s) Transmission lines, busses and transformers associated with such generation	Centrally controlled UFLS system EMS SCADA Generation control system Protective relay Plant control room(s)

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Voltage Support/Reactive Power Supply	Single resource or combined resources (sharing a common mode failure) whose loss or compromised operation may result in: – Unacceptable system voltages – Voltage collapse – Not meeting Nuclear Plant Interface Requirements	Static VAr Compensator Capacitor bank(s) Synchronous Condenser(s) Generation Unit(s) Transmission lines, busses and transformers associated with the such generation	Automated Control System SCADA RTU Protective Relay
Constraint Management	Single resource or combined resources (sharing a common mode failure), transmission facilities or Special Protection Systems whose loss may reduce or eliminate the ability to manage to System Operating Limits or whose compromise could even be used to aggravate constraint loading.	Static VAr Compensator Capacitor bank(s) Synchronous Condenser(s) Generation Unit(s) Transmission lines, busses and transformers	EMS SCADA Automated Substation Control Protective Relays RTUs

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
Control and Operation	Primary and back-up Control Centers, and associated remote data acquisition systems, owned, operated, or employed by Balancing Authorities, Transmission Operators, Generation Operator or Reliability Coordinators that have been registered in the NERC registry Systems essential for reliable BES operation: Inter-utility data exchange Supervisory control or data acquisition Control centre functionality	RC, BA, and TOP Control Centers Generation Control Center	EMS SCADA AGC ICCP RTU
Situational Awareness	Systems essential for reliable BES operation: providing information used to make operational decisions regarding reliability or operability of the BES	– Status or alarm collection – Aggregation – Display functions of a primary or Back-up Control Center – Advanced Network Application (State estimation, Real-time contingency analysis)	– Status or alarm collection – Aggregation – Display functions of a primary or Back-up Control Center – Advanced Network Application (State estimation, Real-time contingency analysis)
Restoration	Generating units, including black-start units; transmission Elements identified in primary cranking paths (including Elements which may not be part of the BES):	Black Start generation unit(s) Reactors, Capacitors Load (distribution	Generation control system SCADA RTU

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
	– which are essential to the initial BES restoration	feeders) Transformers Transmission Lines	Protective Relays
System Stability	Generation resources, transmission facilities and Special Protection Systems whose loss or compromise may result in: – IROL violation – Voltage collapse (wide-spread) – Frequency collapse – Complete operational failure or shutdown of the transmission system – Separation or cascading outages that affect a wide-area spread are of the BES	Transmission lines impacting IROL(s) Generating Unit(s) supporting frequency (with large governor response)/voltage stability/supporting on constraint management on IROLs Capacitor bank(s) Static VAR compensator(s) Synchronous Condensers	Generation control system Associated control systems Protective relays
Load Management	Systems essential to load management whose loss or compromise may impact reliable BES operation: – Demand-Side Management Direct Control Load Management	Load control • Water heater, ac, etc. Interruptible loads DSM Systems Smart Grid	Load Management control system and associated cyber communications
Other	Specific use systems whose loss or compromise may impact the reliable BES operation	Dynamic Feeder Management System Support systems used to modify cyber systems	Dynamic Feeder Management System Support systems used to modify cyber systems

BES Function	BES Subsystem Criteria	BES Subsystem Examples	Cyber System Examples
		(e.g., remote access, relay setting change) Dynamic Ratings monitoring Physical Security System	(e.g., remote access, relay setting change) Dynamic Ratings monitoring Physical Security System

D. IDENTIFICATION OF BES SUBSYSTEMS

The list of BES functions identified above is used to identify all BES Subsystems that support them. The inclusive list of these identified BES Subsystems constitute the overall scope for application of pre-defined criteria for their mapping to categories based on their impact on the reliability or operability of the BES, as defined by the characteristics of an ALR.

While many functions necessary to maintaining an ALR use specific BES elements or facilities, cyber systems may perform or support functions on a wide-area basis. These wide-area cyber systems may be associated with supporting a class of BES Subsystems in aggregate, or may not be associated with any specific BES asset, but directly perform a function necessary to maintain the ALR. Due to the wide-area Cyber System's direct impact on the operability or reliability of the BES, the wide-area Cyber System will be categorized both as a BES Subsystem, to capture the reliability impact, and as a Cyber System, to capture the cyber impact to the function. A centralized, automated, programmable area load shedding system is an example of a system that would be categorized both as a BES Subsystem and as a Cyber System.

Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. For example, a control system in a small generating facility may have a different reliability impact on the BES than an identical control system operating a larger or several generating facilities.

E. IMPACT MAPPING OF BES SUBSYSTEMS

Identified BES subsystems are mapped into categories based on pre-defined criteria that reflect their impact on the reliability or operability of the BES; this mapping will be based on pre-defined criteria, in the functions they provide or support, which determines the level of that impact. As an example, a mapping process to categorize BES subsystems into High, Medium, and Low based on impact could be patterned after criteria used in categorizing bulk power events, such as NERC's Bulk Power System Event Classification Scale, which includes a graduated impact-scale based on: loss of transmission, generation or load; frequency or voltage deviation; BES system separation; and BES system stability. The categorization would also include impacts based on cyber systems, such as situational awareness or operational control.

The work in defining the detailed criteria and categorization levels for mapping of BES subsystems is underway by another Standards Drafting Team subgroup with expertise in BES planning and operating areas.

F. IDENTIFICATION OF BES CYBER SYSTEMS

Once the BES Subsystems have been mapped into the categories based on pre-defined criteria reflecting their impact on the BES, and all the essential functions performed by the BES Subsystems have been identified, the Responsible Entity uses this list to define those BES Cyber Systems that will support:

- The operation and control of these BES Subsystems

  Examples of these are HMI systems in Generating Stations and Transmission Substations, Generating Plant DCS systems, RTUs and PLCs with control and operation functions for BES elements, EMS systems providing control and operate functions for operators

- The monitoring and alerting functions for the reliability or operability of these BES Subsystems

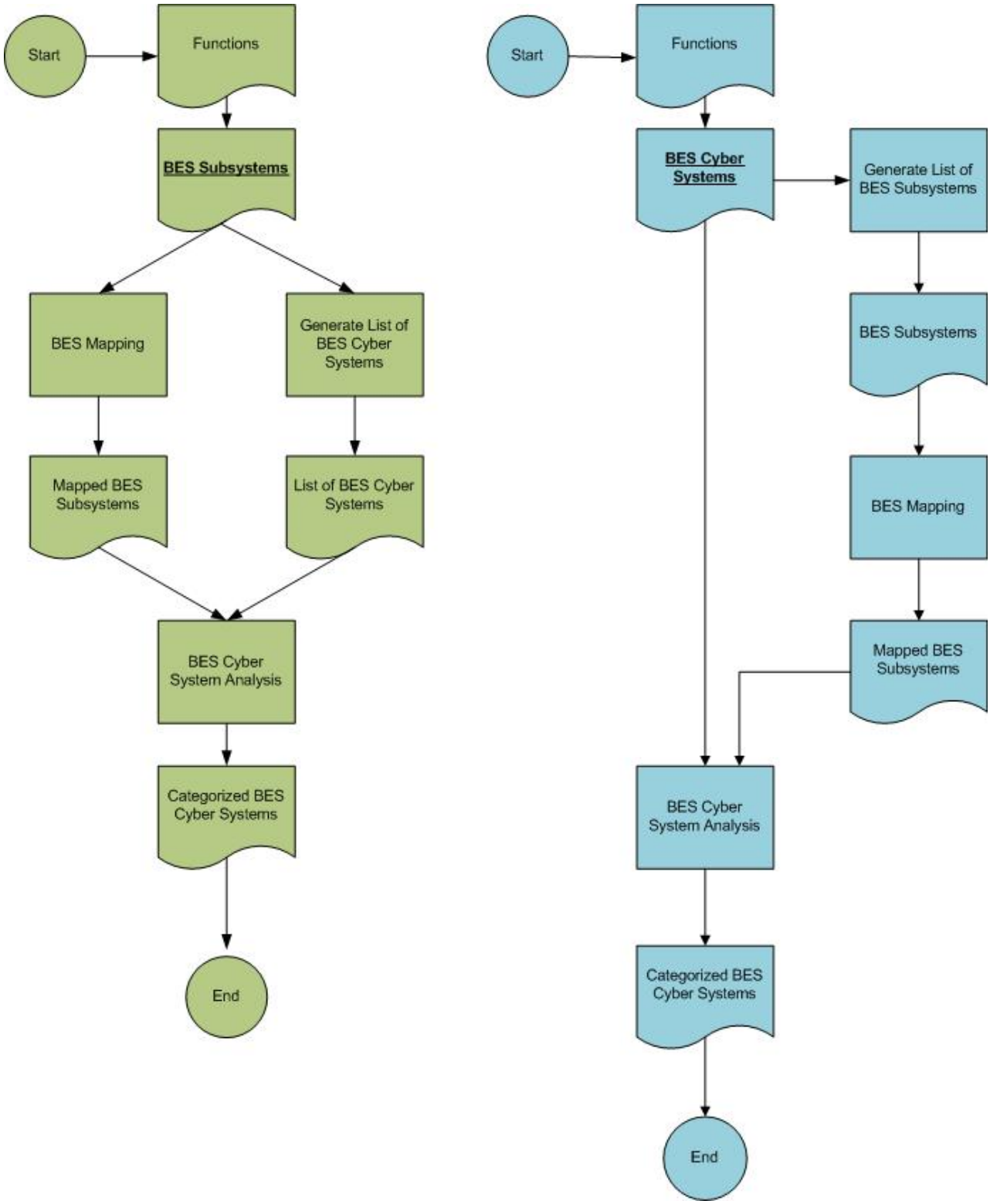
  Examples of these are RTUs providing remote metering functions, Dynamic Feeder Rating systems

- The data acquisition equipment and systems that support wide-area situation awareness for automated or operator assisted real-time reliable operation of these BES Subsystems

  Examples include Phasor Measurement Units when used in State Estimators for real-time operator assisted actions/alerts.

The approach described in this concept paper relies on initially identifying the BES subsystems, then mapping them to pre-defined criteria, and finally categorizing the associated BES cyber systems. Entities may choose to use an alternative approach of: inventorying all their BES cyber systems; analyzing them based on the criteria defined in BES impact mapping of the BES subsystems they support; and utilizing the categorization methodology described later. Both result in the set of categorized BES cyber systems for application of requirements or controls. In both approaches, the BES mapping process is required to determine the impact on the BES.

Figure 2


Start
Functions
BES Subsystems
BES Mapping
Generate List of BES Cyber Systems
Mapped BES Subsystems
List of BES Cyber Systems
BES Cyber System Analysis
Categorized BES Cyber Systems
End
Start
Functions
BES Cyber Systems
Generate List of BES Subsystems
BES Subsystems
BES Mapping
Mapped BES Subsystems
BES Cyber System Analysis
Categorized BES Cyber Systems
End

The focus of this impact categorization is on BES Cyber Systems since they directly support the reliability functions of the BES, but the process does not preclude consideration of other Cyber System components. Determining the full Target of Protection is an important step prior to applying security controls, and its impact categorization is inherited from the BES Cyber Systems within.

G. CATEGORIZATION OF CYBER SYSTEMS

The proposed criteria for the categorization of BES Cyber Systems are based on their impact on the functions of the BES Subsystems they support. For each BES Cyber System, a Responsible Entity determines the impact of the loss of confidentiality, integrity, and availability resulting from its loss or compromise to the functions of the BES Subsystem it supports. Categories of impact are defined as follows:

- **High** if the loss of confidentiality, integrity, or availability directly causes or contributes to the loss or compromise of the integrity or availability of the BES Functions it supports.
- **Medium** if the loss of confidentiality, integrity, or availability directly affects the BES Functions it supports, but is unlikely to lead to the loss or degradation of operational integrity or availability of the functions.
- **Low** if the loss of confidentiality, integrity, or availability would not be expected to affect the BES Functions it supports.

This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES Subsystems as shown in Figure 3. For example, a SCADA system may provide automated generation control signals to a generator with minimal impact on the BES. However, the same SCADA system also provides control for substations on a high impact transmission line. As a result, the Responsible Entity would assign the final security categorization as *High* for the SCADA system.

This categorization approach makes two important advancements to ensuring a more complete and accurate assessment of Cyber System impact on the BES. First of all, the impact analysis requires a consideration of the functions of the BES Subsystem it supports. Secondly, the categorization ties directly to the security requirements of the Cyber System. As a result, the later security control selection should have its basis in reducing risk to the BES caused by a

Cyber Security Incident.

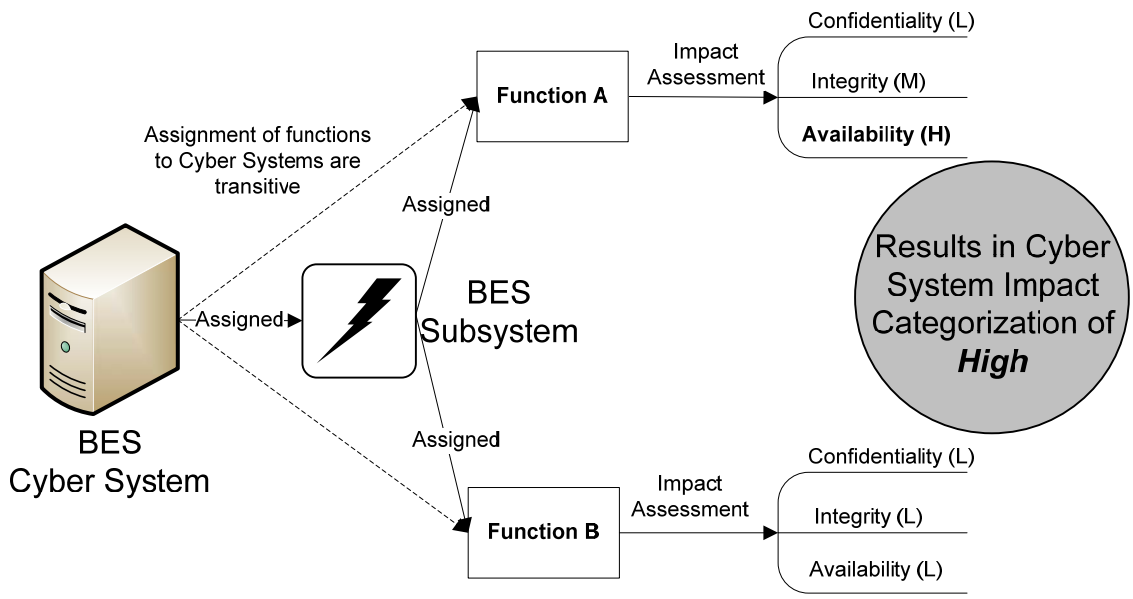


Figure 3: Cyber System Security Impact Categorization

H. FINAL CATEGORIZATION OF CYBER SYSTEMS BASED ON OVERALL IMPACT ON THE BES

The final categorization of each cyber system is determined by a matrix which has predetermined outcomes. The pre-determined categorization of the cyber system is based on both the impact mapping of the supported BES Subsystem and the impact of the cyber system on the BES function it supports.

This deterministic methodology will provide a more consistent approach and result than the looser requirement of a risk-based methodology included in CIP-002-1 and CIP-002-2. The approach is based on an impact based methodology and will provide for more uniform application of a methodology for categorizing cyber systems.

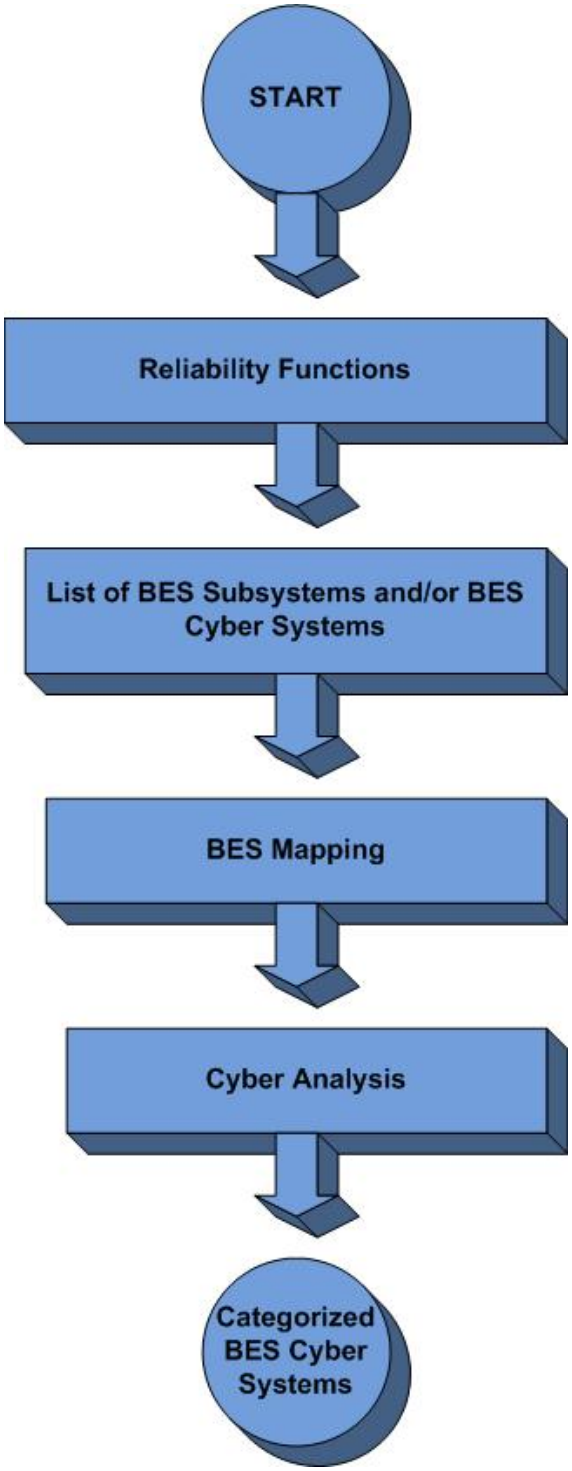
An example of the application of this approach in an evaluation matrix is shown below:

> **Note:** *Table 2 is a visual representation of what the categorization can look like, it's not the actual table.*

Table 2

Asset Impact -->	**High**	**Medium**	**Low**
Cyber Impact:			
High	H	H	H
Medium	H	M	M
Low	H	M	L

Figure 4


START
Reliability Functions
List of BES Subsystems and/or BES Cyber Systems
BES Mapping
Cyber Analysis
Categorized BES Cyber Systems

I. DEFINING THE TARGET OF PROTECTION

Up to this point, the process being laid out has focused on determining the impact that BES Cyber Systems have on the BES. The process now shifts to the Responsible Entity **protecting** the BES Cyber Systems; this begins with defining the set of both BES and non-BES Cyber Systems that must be protected to provide an adequate level of protection to the BES Cyber Systems. This resulting set of Cyber Systems is defined as the *Target of Protection*, to which a Responsible Entity would apply appropriate security controls.

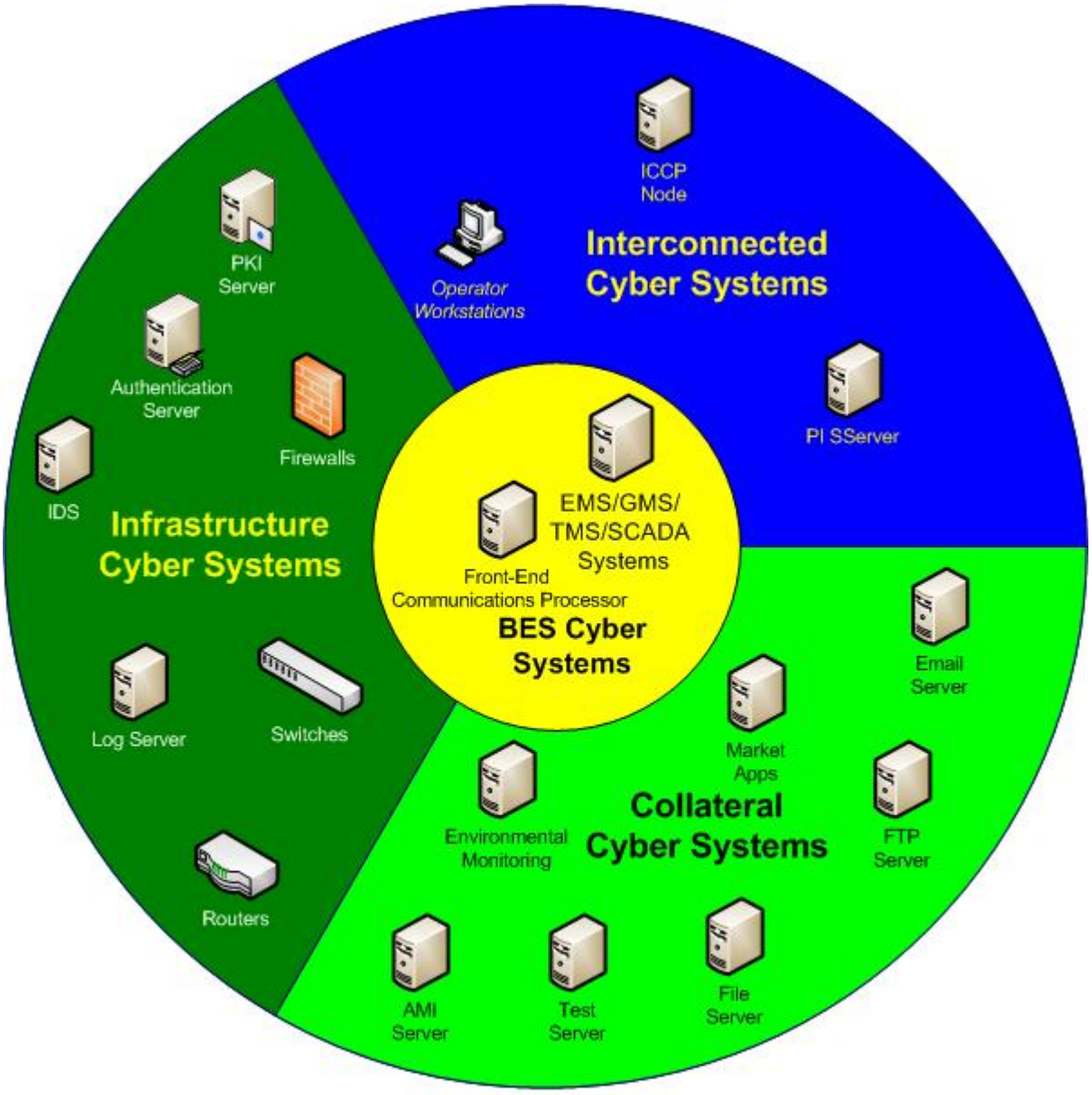
To form the Target of Protection, the Responsible Entity would start with the BES Cyber System and determine any additional *Interconnected Cyber Systems* supporting the mapped BES function(s). These Interconnected Cyber Systems may have involvement with the exchange and display of data but do not necessarily perform the BES function(s) themselves. Examples include historical data collectors, ICCP Nodes, Operations Support Workstations, etc. It is important to stress that these interconnected Cyber Systems may both exist outside of the traditional Electronic Security Perimeter and be operated external to a Responsible Entity. Those third-party interconnected Cyber Systems are discussed further in the next section.

In addition to the identified interconnected cyber systems, the Responsible Entity would also determine those Cyber Systems supporting the confidentiality, integrity, availability and non-repudiation requirements of the BES and Interconnected Cyber Systems. Examples of these may include routers, switches, firewalls, components involved in access-control and/or security monitoring, virtual server management, environmental control and/or monitoring systems.

A final class of Cyber Systems is incorporated within the Target of Protection only on the basis of their locality within a network segment or operating environment. The Responsible Entity can remove these *Collateral Cyber Systems* from the operating environment with no significant effect to the BES function, but an attacker could utilize its otherwise relaxed security posture to attack the function. As an example, an email server, while not supporting the BES function, may be located on the same network segment as the Interconnected or Infrastructure Cyber Systems. This introduces an unnecessary vulnerability and should be moved out of that network segment.

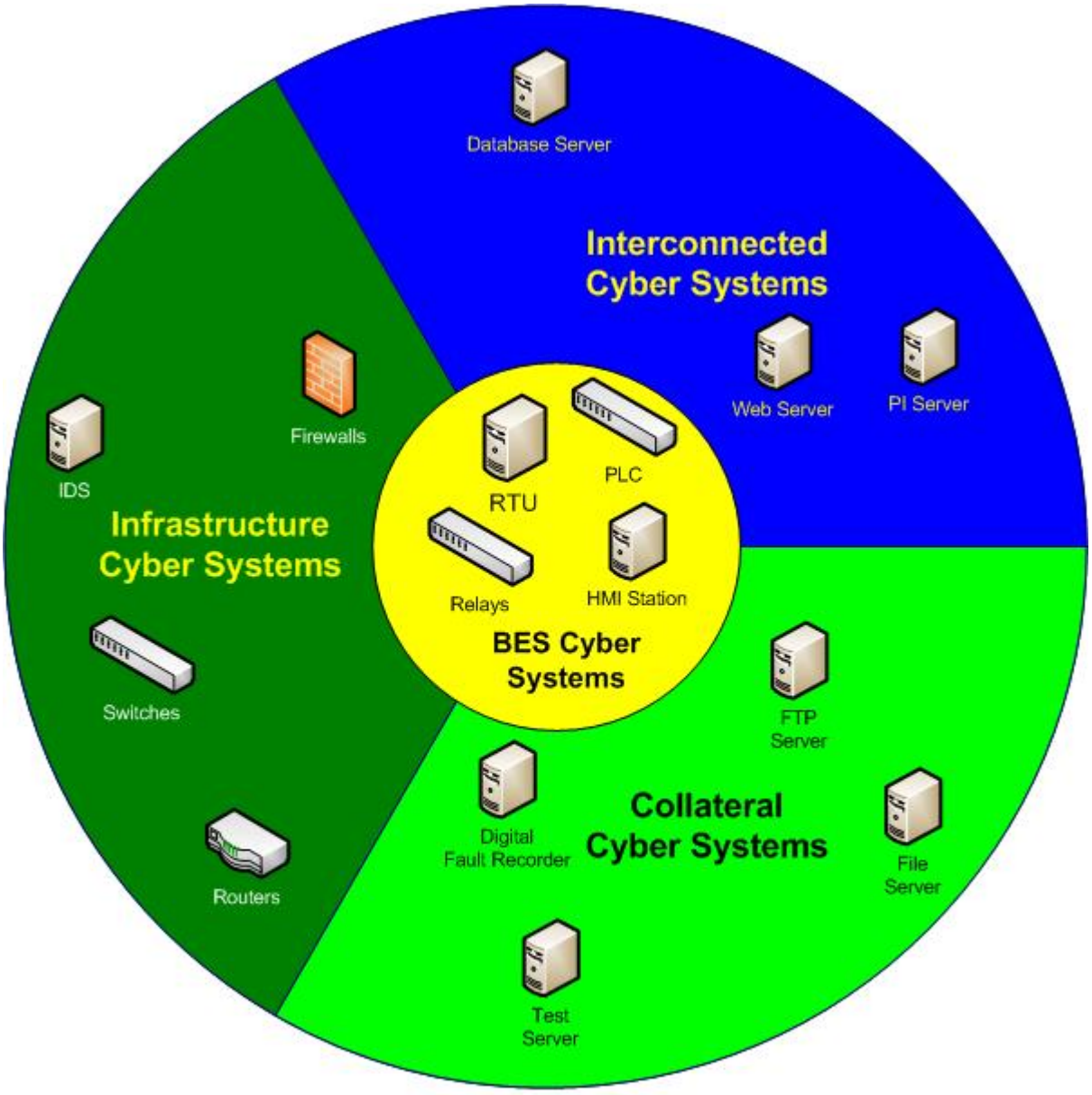
Examples of defining the Target of Protection are illustrated in the following diagrams. The systems in these figures are only specified for representation and may differ based on their functional role associated with the BES Cyber System.

Figure 5



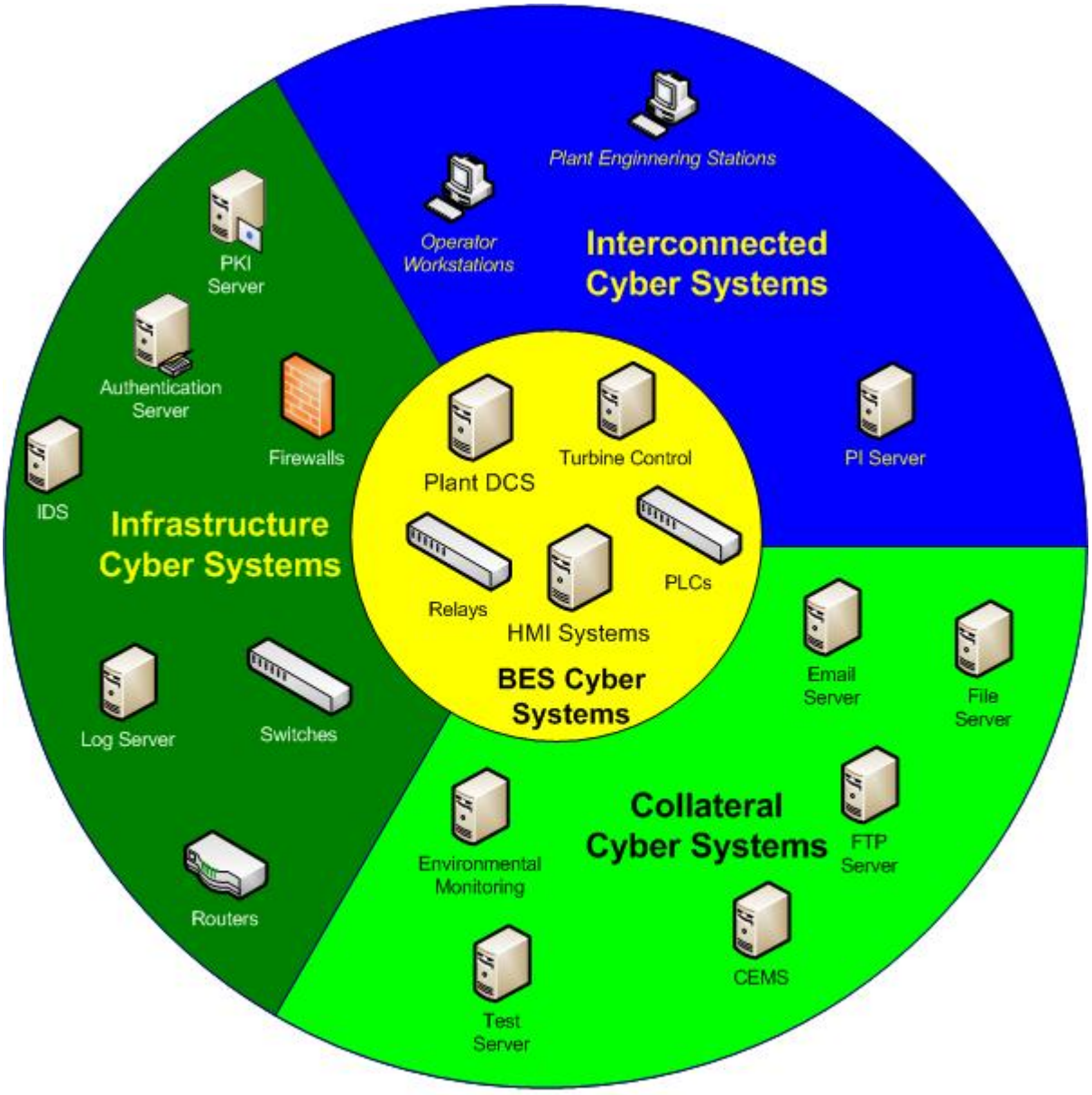
Target of Protection – Control Center

Figure 6



Target of Protection – Transmission Substations

Figure 7



Target of Protection – Generation

A Responsible Entity has flexibility in defining a Target of Protection to maximize efficiency in secure operations. They may choose the definition to include all Cyber Systems responsible for carrying out a single function or they may define it based on network proximity. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly would make the secure operation difficult to monitor and assess. To determine the Target of Protection, the Responsible Entity would take into account the operational environment and scope of management.

As an example, consider the following diagrams. A Responsible Entity may declare the entire SCADA cyber system to include supervisory control servers and field devices or multiple, similarly designed substation networks as a single Cyber System. This may make sense if they all lie under the same operational management. Or it may choose to define the few essential components in a substation network as the Cyber System.

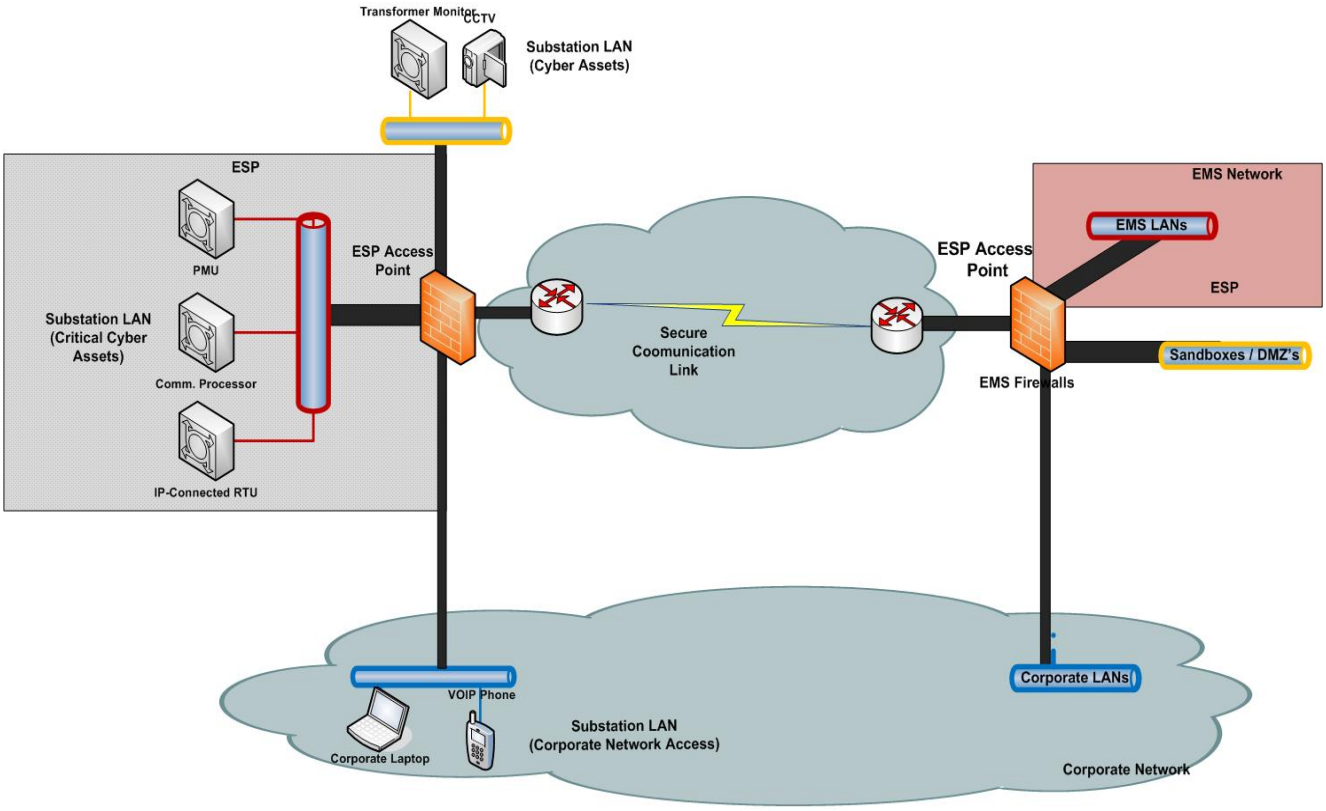


Figure 8 — SCADA and Substation Cyber System — Separate Security Perimeters

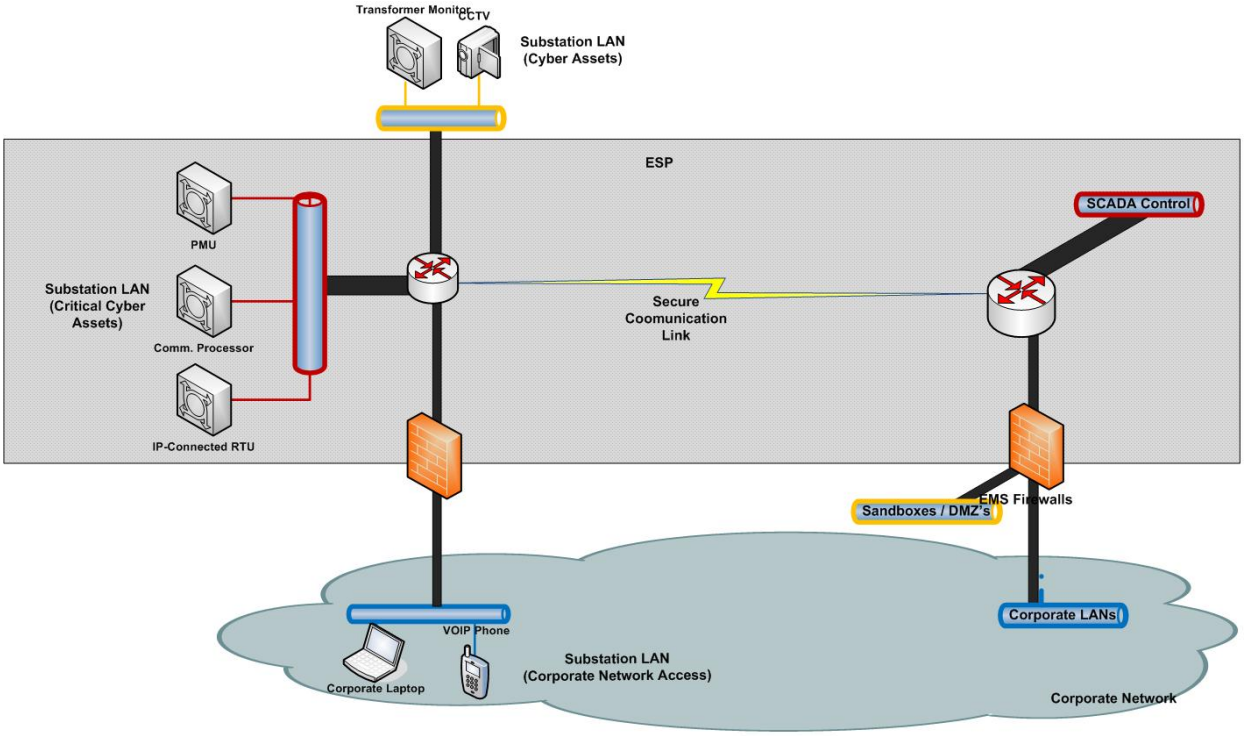


Figure 9 — SCADA and Substation Cyber System — Single Security Perimeter

J. EXTERNAL CYBER SYSTEMS

Cyber Systems performing functions of the BES exist within a complex network of interconnections and information exchange across multiple organizations. Just as a downstream fault could cause cascading power outages, so too, a compromise of one Cyber System could utilize a trusted path to impact multiple other Cyber Systems. Consequently, to achieve the desired protection level in the BES Cyber System, these external party dependencies cannot be ignored in establishing the Target of Protection.

As components of the Target of Protection cross organizational boundaries, the Responsible Entity with operational responsibility for the BES Cyber System should identify and manage the risk of these dependencies. This would include the identification of third party service providers operating within the Target of Protection, but it may also include a third party data connection outside of the traditional Electronic Security Perimeter.

As an example, if Utility Alpha categorizes one of its Cyber Systems as High and identifies an external interconnection with Company Beta as part of the Target of Protection, then Utility Alpha owns the risk associated with the interconnection and has the responsibility to mitigate the risk.

This approach ensures the standards consider the complex nature of Cyber Systems to protect the reliability or operability of the BES and assist organizations operating Cyber Systems downstream to understand their impact on the BES.

K. APPLYING SECURITY CONTROLS TO THE TARGET OF PROTECTION

At this point in the process, a Responsible Entity has assigned an impact category to a Cyber System and determined their Target of Protection. Now the remaining task involves mitigating the risk posed to the BES by applying an appropriate set of security controls and requirements to the Target of Protection. A crucial undertaking for the drafting team lies in developing these security controls in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry.

To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed. A part of this effort involves utilizing the impact categorization process. The underlying assumption for categorizing BES Cyber Systems is the need for differing levels of protection.

The application of security controls will consider the differences in contexts and characteristics in transmission substations, generating plants and control centers, their cyber equipment types and operating environments, and evaluate an approach to protect them without unduly requiring entities to invoke exception processes in the standards.

In the drafting of the controls and requirements, the drafting team will consider approaches to provide flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities. The drafting team will seek industry comments in the area of control specifications in future papers.

L. CONCLUSION

The approach proposed in this paper builds on work that the industry has already done in complying with the current standards, the guidance to be available soon in using a risk-based methodology for classifying BES Subsystems, the industry's experience and investments in current compliance programs, and a recognition that the reliability of the BES is based on an engineered system increasingly supported by cyber systems. It is an approach that represents a new paradigm and addresses many areas of the perceived or real deficiencies in the current CIP-002 standard. It seeks to ensure that all cyber systems related to the reliability or operability of the BES are required to implement a security posture commensurate to the level of criticality of the BES Subsystems they are supporting.

APPENDIX A: TERMS AND DEFINITIONS

Appendix A provides the defined terminology used throughout this concept paper. These terms are ordered here hierarchically to build upon each other and culminate to a definition of what the NERC Cyber Security Standards should seek to protect.

BES Subsystem	The set of BES assets necessary to perform or support a function or set of functions necessary to maintain an Adequate Level of Reliability in the Bulk Electric System. A BES Subsystem may be defined as a piece of equipment, a facility or system.
Cyber Asset [NERC Glossary]	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber System	A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (It is important to note the term system is used by itself in places throughout this paper and should not be considered interchangeable with Cyber System. A system performing a reliability function of the BES may be either electromechanical, manual or cyber in nature.)
BES Cyber System	A Cyber System directly supporting reliability functions of the BES. The term *BES* distinguishes the Cyber System from those which do not directly relate to a BES function for the purpose of simplifying the categorization process. Examples of *BES Cyber Systems* may include SCADA/EMS systems, generation DCS, RTU providing control, or HMI Workstations.
Interconnected Cyber Systems	Components necessary for BES *Cyber Systems* to perform their BES functions. These Cyber Systems may have involvement with the exchange and display of data but do not perform the BES functions themselves. Examples include historical data collectors, ICCP nodes or operations support workstations.
Infrastructure Support Cyber Systems	Components supporting the confidentiality, integrity, and availability of the BES and *Interconnected Cyber Systems*. Examples include routers, switches, firewalls, components involved in access-control and/or security monitoring, virtual server management, and environmental control and/or monitoring systems.

Collateral Cyber Systems	Other components included in the *Target of Protection* only on the basis of their locality within a network segment or operating environment.
Target of Protection	A Cyber System consisting of all components necessary to evaluate the desired level of resiliency in the BES functions the Cyber System provides and/or allows.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

July 21, 2009

TO: INDUSTRY STAKEHOLDERS

RE: REQUEST FOR INFORMAL INDUSTRY COMMENT REGARDING THE APPROACHES IN THE CONCEPT PAPER "*CATEGORIZING CYBER SYSTEMS — AN APPROACH BASED ON BES RELIABILITY FUNCTIONS*"

Ladies and Gentlemen:

In 2008, the Federal Energy Regulatory Commission (FERC) issued Order 706 paragraph 236 directing the Electric Reliability Organization (ERO) to develop modifications to Reliability Standard CIP-002-1 — Cyber Security — Critical Cyber Asset Identification to address its concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal management approval of the risk-based assessment; (4) the external review of critical assets identification; and (5) interdependency analysis.

On August 7, 2008, the NERC Standards Committee appointed a standards drafting team (SDT) to develop these modifications as part of Project 2008-06 — Cyber Security Order 706. The SDT for the project (CS 706 SDT) was charged to review each of the critical infrastructure protection (CIP) standards and address the modifications identified in FERC Order 706.

CIP-002-2 — Cyber Security — Critical Cyber Asset Identification provides the foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After deliberation, the CS 706 SDT is proposing to revise CIP-002-2 — Cyber Security — Critical Cyber Asset Identification to require a methodology that categorizes BES subsystems and cyber systems according to their impacts on reliability functions. This significant change will benefit the industry by:

- preserving most, if not all, the previous work to protect Critical Cyber Assets under the existing CIP standards;
- eliminating the one-size-fits-all deficiencies of the existing standards;
- simplifying and making uniform the process of asset identification and classification;
- eliminating the need for third-party asset identification oversight;
- improving the overall cyber security of BES assets; and
- minimizing the number of Technical Feasibility Exceptions that an entity would otherwise require for compliance.

This approach is outlined in the concept paper *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*. The concept paper proposes a broader and more comprehensive cyber security approach to protect the systems that support a reliable BES as compared to the requirements contained in the current CIP-002-2 — Cyber Security — Critical Cyber Asset Identification standard.

The CS 706 SDT is seeking informal industry comment on the approaches presented in the concept paper. The CS 706 SDT is requesting comments and suggestions regarding four areas in particular:

- BES reliability functions
- identification of BES subsystems and BES cyber systems
- mapping of BES subsystems
- categorization of cyber systems

Industry input is also requested on the methodology for identification of a "library of security protections" that may be applied to mitigate the risks to the BES.

The informal industry feedback comments provided in response to this posting will be considered by the CS 706 SDT and incorporated, as appropriate, in developing the CIP-002 draft requirements. In the interest of focusing available resources on CIP Version 3 standards development, the SDT will not formally respond to the comments. A subsequent draft CIP-002 — Cyber Security — Cyber Systems Categorization standard will be posted for formal industry comment as part of the ANSI formal standards development process later this year.

The readers of the concept paper are encouraged to use all of their experience during their review, but should be prepared to have their assumptions challenged, as the concepts presented represent a paradigm shift for experienced operating personnel. Cyber security inherently concerns more than a piece of hardware or software or a communication circuit; it encompasses the *system* intimately associated with the reliability functions that it supports.

Due Date and Submittal Information:
The informal comment period is open **until 8 p.m. EDT on September 4, 2009**. Please use this Word form to submit comments. If you experience any difficulties in using the Word form, please contact Lauren Koller at Lauren.Koller@nerc.net. The informal comment form and concept paper is posted on the project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

Consolidation of Comments

Cyber Security Concept Paper:
"Categorizing Cyber Systems — An Approach Based on BES Reliability Functions"

This Consolidation of Comments summarizes the comments received during the 45 day industry comment period for the Cyber Security Concept Paper: "*Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*," developed by the Project 2008-06 — Cyber Security Order 706 Standards Drafting Team (CS 706 SDT).

The 45-day comment period began on July 21, 2009 with an email industry stakeholders from NERC staff. Commenters were to email their comments to NERC staff at sarcomm@nerc.net by September 4, 2009 with the following subject line: "**Categorizing Cyber Systems Comment Form**".

As shown in Table 1, Listing of Commenters, question responses and comments on the subject concept paper were received from 52 sets of commenters. These question responses and comments have been forwarded to the CS 706 SDT to assist then in developing Reliability Standards Requirements for the next version of Standard CIP-002.

Comments were solicited from industry in response to 11 specific questions, as well as general editorial comments on the concept paper itself. This document represents a consolidation of all comments received. All comments are identified by a unique commentor identifier.

Responses to the questions are grouped by question, and presented in the same order as the commentors are listed in Table 1. Some commentors elected to only comment on a subset of the sections. If a commentor did not submit a comment for a particular section, no reference to that commentor is included in that section.

Comments submitted as general editorial comments to the concept paper are ordered by the section page number and line number to which the comment relates, thereby grouping like comments together. Some commentors elected to not provide general edit comments. No indication is provided for non-commentors to this section.

Table 1 – Listing of Commenters

Cyber Security Concept Paper: "*Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*"

		Commenter	Organization	Identifier
1.	Individual	Steve Alexanderson	Central Lincoln People's Utility District	CLPUD
2.	Individual	David Martorana	Tenaska, Inc.	TNSK
3.	Individual	Bill Hellinghausen	Eagle Energy Partners	EAGLE
4.	Individual	Alice Murdock	Xcel Energy	XCEL
5.	Group	Ruth Blevins	Virginia Electric and Power Company	DOM
		John Calder	Virginia Electric and Power Company	
		Vern Colbert	Virginia Electric and Power Company	
		Marvin Walker	Virginia Electric and Power Company	
		Louis Slade	Virginia Electric and Power Company	
		Michael Gildea	Virginia Electric and Power Company	
		Mike Garton	Virginia Electric and Power Company	
		Connie Lowe	Virginia Electric and Power Company	
		Dennis Sollars	Virginia Electric and Power Company	
		Paul Rodi	Virginia Electric and Power Company	
		Dan Goyne	Virginia Electric and Power Company	
		Linda Krepp	Virginia Electric and Power Company	
		Perry Esposito	Virginia Electric and Power Company	
		Chip Humphrey	Virginia Electric and Power Company	
		George Wood	Virginia Electric and Power Company	
		Randy Reynolds	Virginia Electric and Power Company	
		John Loftis	Virginia Electric and Power Company	
		John Rainey	Virginia Electric and Power Company	

		Commenter	Organization	Identifier
		Marc Gaudette	Virginia Electric and Power Company	
		Dave Connelly	Virginia Electric and Power Company	
		Karen Curtis	Virginia Electric and Power Company	
		Jalal Babik	Virginia Electric and Power Company	
		Johmar Frias	Virginia Electric and Power Company	
6.	Individual	Frank Gaffney	Florida Municipal Power Agency and Some Members: Lakeland Electric, Beaches Energy Services, Kissimmee Utility Authority, Fort Pierce Utility Authority, and City of Vero Beach	FMPA
7.	Individual	Gary W. Cox	Southwestern Power Administration	SWPA
8.	Individual	John Brockhan	CenterPoint Energy	CPE
9.	Individual	Anthony Wright	Georgia Transmission Corporation	GTC
10.	Individual	Ron Blume	Dyonyx	DYONYX
11.	Group	Denise Koehn	Bonneville Power Administration	BPA
		Curt Wilkins	Bonneville Power Administration	
		Kelly Hazelton	Bonneville Power Administration	
		Huy Ngo	Bonneville Power Administration	
		Kelly Gardner	Bonneville Power Administration	
		Pete Raschio	Bonneville Power Administration	
		Sharon Brown	Bonneville Power Administration	
		Karin Butler	Bonneville Power Administration	
		Kevin Dorning	Bonneville Power Administration	
		Laura Demory	Bonneville Power Administration	
		Rita Coppernoll	Bonneville Power Administration	
12.	Individual	Dave Batz	Edison Electric Institute	EEI
13.	Individual	Randy Schimka	San Diego Gas and Electric Co.	SDGE

		Commenter	Organization	Identifier
14.	Individual	Guy Andrews	Georgia System Operations Corp.	GSOC
15.	Individual	Ed Carmen	Baltimore Gas and Electric Company	BGE
16.	Individual	John Allen	City Utilities of Springfield, Missouri	CUSMO
17.	Group	Greg Fraser	Manitoba Hydro	MH
		Jackie Collett	Manitoba Hydro	
18.	Group	Roger Fradenburgh	Network & Security Technologies, Inc.	NST
		Nick Lauriat	Network & Security Technologies, Inc.	
		Nic Ziccardi	Network & Security Technologies, Inc.	
19.	Group	Guy Zito	Northeast Power Coordinating Council	NPCC
		Ralph Rufrano	New York Power Authority	
		Alan Adamson	New York State Reliability Council, LLC	
		Gregory Campoli	New York Independent System Operator	
		Roger Champagne	Hydro-Quebec TransEnergie	
		Kurtis Chong	Independent Electricity System Operator	
		Sylvain Clermont	Hydro-Quebec TransEnergie	
		Manuel Couto	National Grid	
		Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	
		Brian Evans-Mongeon	Utility Services	
		Mike Garton	Dominion Resources Services, Inc.	
		Brian L. Gooder	Ontario Power Generation Incorporated	
		Kathleen Goodman	ISO - New England	
		David Kiguel	Hydro One Networks Inc.	
		Michael R. Lombardi	Northeast Utilities	
		Randy MacDonald	New Brunswick System Operator	

		Commenter	Organization	Identifier
		Greg Mason	Dynegy Generation	
		Bruce Metruck	New York Power Authority	
		Chris Orzel	FPL Energy/NextEra Energy	
		Robert Pellegrini	The United Illuminating Company	
		Michael Schiavone	Nation Grid	
		Peter Yost	Consolidated Edison Co. of New York, Inc.	
		Gerry Dunbar	Northeast Power Coordinating Council	
		Lee Pedowicz	Northeast Power Coordinating Council	
20.	Group	Larry Bugh	ReliabilityFirst Corporation	RFC
		Lew Folkerth	ReliabilityFirst Corporation	
		Steve Garn	ReliabilityFirst Corporation	
21.	Group	Jim Brenton	ISO/RTO Council—Security Working Group	IRC
		Ann Delenela	ERCOT	
		Joe Pereira	ISO-NE	
		David Dunn	IESO	
		James Sample	TVA	
		John McGlynn	PJM	
		Philip Propes	SPP	
		Christine Hasha	ERCOT	
		Ann Delenela	ERCOT	
		Jason Marshall	MW-ISO	
		Jeff Maddox	ERCOT	
		Tim Lockwood	Cal-ISO	
22.	Group	Doug Hohlbaugh	FirstEnergy	FE

		Commenter	Organization	Identifier
		Rob Martinko	FirstEnergy	
		John Olszewski	FirstEnergy	
23.	Individual	Thad Ness	American Electric Power	AEP
24.	Individual	Joseph G. DePoorter	Madison Gas and Electric Company	MGE
25.	Individual	William Lucas	Wisconsin Electric Power Company	WE
26.	Individual	Eric Scott	Ameren	AMEREN
27.	Individual	Laura Lee	Duke Energy	DUKE
28.	Group	Hugh Francis	Southern Company	SOCO
29.	Individual	Robert Tallman	E.ON U.S.	E-ON
30.	Individual	Jason Shaver	American Transmission Co.	ATC
31.	Individual	Terri Pyle	Oklahoma Municipal Power Authority	OMPA
32.	Group	William Gallagher	Transmission Access Policy Study Group (TAPS), representing transmission dependent utilities in more than 35 states	TAPS
33.	Group	Katherine Hamilton	GridWise Alliance, Interoperability/Cyber Security Work Group	GWA
34.	Individual	Jason L. Marshall	Midwest ISO	MISO
35.	Individual	Jamie Starling	SCE&G	SCEG
36.	Group	Dan Powell	ReliabilityFirst CIP Committee (RFC CIPC)	RFC-CIP
			Indianapolis Power & Light Company	
		Mark Stefaniak	DTE Energy	
37.	Group	Sheryl Byrd	GE Energy Infrastructure	GEEI
		Matt Thomson	GEEI	
		Barry Littlefield	GEEI	
		Robert Boring	GEEI	
		Doug Cole	GEEI	

		Commenter	Organization	Identifier
		Dietmar Breitkreuz	GEEI	
		Daiane Carneiro	GEEI	
		Holly Chase	GEEI	
		Ruben Altunian	GEEI	
		Missam Momin	GEEI	
		Lisa Whelchel	GEEI	
		Charlie Campione	GEEI	
		James Fealey	GEEI	
		Gary Gray	GEEI	
		Jack Shoffstall	GEEI	
		George Runkle	GEEI	
		Martha Saker	GEEI	
38.	Individual	Paul Crist	Lincoln Electric System	LUS
39.	Group	Carol Gerou	MRO NERC Standards Review Subcommittee	MRO
		Neal Balu	Wisconsin Public Service	
		Terry Bilke	Midwest ISO	
		Ken Goldsmith	Alliant Energy	
		Jodi Jensen	Western Area Power	
		Terry Harbour	MidAmerican Energy Company	
		Joe Knight	Great River Energy	
		Alice Murdock	Xcel Energy	
		Scott Nickels	Rochester Public Utilities	
		Dave Rudolph	Basin Electric Power Cooperative	
		Eric Ruskamp	Lincoln Electric System	

		Commenter	Organization	Identifier
40.	Individual	Steve Newman	MidAmerican Energy Company	MEC
41.	Individual	Chris Klemm	PSEG	PSEG
42.	Individual	Shawn Barrett	Michigan Public Power Agency	MMPA
43.	Individual	Robert J. Kang	Southern California Edison	SCE
44.	Individual	Michael Goggin	American Wind Energy Association	AWEA
45.	Individual	Allen Mosher	American Public Power Association	APPA
46.	Individual	Paul Golden	PacifiCorp	PAC
47.	Individual	Martin Bauer	Bureau of Reclamation	USBR
48.	Individual	Mike McClain	Portland General Electric Co.	PGE
49.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	BRAZOS
50.	Individual	Chantel M. Haswell	Florida Power & Light	FPL
51.	Individual	Robert S. Lynch	Southwest Transmission Dependent Utility Group representing: Aguila Irrigation District, Ak-Chin Energy Services, Buckeye Water Conservation and Drainage District, Central Arizona Water Conservation District, Electrical District No. 3, Electrical District No. 4, Electrical District No. 5, Electrical District No. 6, Electrical District No. 7, Electrical District No. 8, Harquahala Valley Power District, Maricopa County Municipal Water District No. 1, McMullen Valley Water Conservation and Drainage District, City of Needles, Roosevelt Irrigation District, City of Safford, Tonopah Irrigation District, Wellton-Mohawk Irrigation and Drainage District	SWTDUG
52.	Individual	Paul McClay	Tampa Electric	TECO

Question 1

Specific Questions:

1. Section C, BES Reliability Functions discusses a categorization approach based on reliability functions. Is the concept of categorizing by function instead of by asset clear? If not why?

Name	Comment
CLPUD	No. It is unclear if an entity starts with owned/operated equipment that is included in the NERC definition of BES and sorts them into the various BES subsystems, or sorts all equipment to see if they fit into the subsystems and assumes if they fit they are included in the BES. If the later is intended, this alters the NERC definition of BES.
TNSK	The Section C, BES Reliability Functions is very clear in that the categorizing will be done by function instead of by asset. This section should also specify that the Regional Coordinator will supply the impact assessment of the BES subsystem as it applies to the Generator Owners and Generator Operators.
XCEL	Yes
DOM	Yes, the concept is clear, but its scope is far too broad. Rather than using a risk based process to identify and focus on critical assets, it appears that this process could require every device used by every utility to be assessed equally. An approach that does not consider potential BES impacts and the probability of their occurrence early in the evaluation process exposes the industry to a very cumbersome risk-based evaluation process that will be extremely resource intensive to the point that it may be difficult to effectively implement and execute. Using load management as just one example of the issues raised by this "all in approach", if smart meters are being utilized, would every smart meter have to be assessed? Also, since there are requirements for load management in other existing reliability standards (i.e.: EOP-001, EOP-002, MOD-002, MOD-006, MOD-019, and MOD-020), which are applicable to many entities (BA, TOP, LSE, RC, TSP, PA, and RP) will each of these entities also have to evaluate smart meters under their jurisdiction against each applicable reliability standard requirement? How will owners of reliability functions be identified? Functions are typically shared by multiple entities and security levels, and protections would need to be coordinated among multiple entities. The owner of each device will also have to be involved in the decisions in determining what protections are required and why. Also, different reliability functions will have different impacts. Will there be a hierarchy of functions and of applicable reliability standard requirements? How will conflicts be resolved if they arise? Under the proposal as Dominion understands it, the entity(ies) responsible for each reliability function will have to play a much larger role in critical asset identification than they do currently. The reliability entity (PJM for the majority of Dominion's assets) will have to evaluate all the BES equipment that contributes to

	reliability and prioritize each piece of equipment's impact on the BES function and cyber vulnerability. This will entail that the reliability entity identify and understand every specific process, procedure and system from every member company (547 Members for PJM) necessary to achieve an adequate level of reliability ("ALR") and communicate these to the owners of all the assets necessary to achieve that ALR. These asset owners would then have to protect the equipment based on the highest evaluation provided by their reliability entities. This may require a much higher level of coordination than is required currently. It is also unclear how market rules may factor into implementation of this concept. Reliability standards contain the term 'load management', however the industry has been encouraged to increase the use of demand response and treat it in a manner similar to a generator. The technology implementing demand response is already being used in capacity markets of various RTOs/ISOs. The growth in this technology is expected to move into all aspects of load balancing and perhaps ancillary services such as regulation and reserves. This could mean that changes to the Functional Model as well as changes to existing, or the development of new, reliability standards and requirements will be needed. As demand response becomes an element of long term planning, the complexities increase. This paper should anticipate questions such as who will 'own' future load management (demand response) end–use customers, and who will determine how CIP standards will be met. There seems to be agreement that the one-size-fits-all approach should be abandoned. However, we are concerned that a literal interpretation of this concept paper as now written implies that every piece of equipment or software in, for example, a power station, substation, and/or control room is involved with reliability. This extreme viewpoint would mean that every device and every piece of software will need to be evaluated. Such evaluations are outside the scope of these CIP standards. Reliability of the BES itself is and should be covered by the other NERC standards already in place. The purpose of these CIP standards should be to protect against cyber attacks. Critical assets (however they are defined and identified) may need higher protection, but the one size-fits-all approach needs to give way to a more practical approach that accomplishes the goal of cyber protection without making it so onerous that owners will find it difficult to comply with the cyber standards themselves.
FMPA	First, let us say that we appreciate the efforts of the SDT to publish a concept paper on this very important topic to gain industry feedback early in the process. We believe the SDT is wise in doing so. Also, FMPA wants to make it clear that we believe that cyber security is essential and we support these important efforts to increase the security of one of our society's vital infrastructures; but, we also believe that these efforts needs to be focused on what is really important so that the efforts are most effective and not overly burdensome to the industry and to the Regional Entities. FMPA also agrees that a "yard-stick" is needed to determine whether a cyber system ought to be regulated by these standards. However, FMPA believes the yard-stick ought to be the definition of reliability as described in the Federal Power Act, Section 215(a)(4): "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements". Section 215 is clearly focused on avoiding "instability, uncontrolled separation, or cascading failure" and not on local impacts. Bearing Section 215's definition of reliability in mind, FMPA believes that an "Adequate Level of Reliability" ("ALR") is not the appropriate yard-

	stick for these standards. FMPA believes that, because these standards apply to "critical" cyber assets, the correct yard-stick is the definition of reliability in Section 215, which essentially refers to avoiding wide-area blackouts, and not the ALR yard-stick which would include local area issues that have no consequence to the wide-area. Using ALR as the yardstick will likely sweep in nearly all cyber systems that touch the BES because entities plan, design and operate the system to achieve ALR without much margin, otherwise there would be an opinion that we are "gold-plating" the system. We do not believe that it is the intent of these standards to regulate all cyber assets, but only those most "critical", meaning a subset of cyber systems that are, using synonyms, indispensible or vital that, if maliciously used, could cause "instability, uncontrolled separation, and cascading outages". FMPA agrees that Risk Management principles are the correct principles to use in determining which cyber systems ought to be regulated by the standards and how. FMPA also agrees that the existing methodology of identifying "critical assets" followed by "critical cyber assets" is flawed and prone to overlooking interactions. However, there are multiple ways to perform a risk management assessment, only one of which is the one proposed by the SDT. The fundamental premise of risk management is: 1) to inventory threats (or risks); 2) to evaluate the impacts of those threats; and 3) to develop methods to address those threats commensurate with their impacts and frequency of occurrence. FMPA believes that the bottom line of the CIP 002 assessment ought to be just that and the method by which an entity gets to the point of inventorying threats ought to be left up to that entity (e.g., the standard ought to regulate the "what", not the "how"). For instance, if the entity wants to define BES Reliability Functions, then BES Subsystems, to then proceed to an inventory of cyber assets and their threats, then, that should be the entity's choice. If another entity wants to proceed directly to inventorying cyber assets and associated threats, then that should be their choice. The standards / concept paper ought to reflect only the bottom line – inventorying threats and their impacts. Developing new definitions and new concepts such as BES Reliability Functions and BES Subsystems adds a level of complexity and overhead costs to the process that is not needed. The SDT might believe that the methodology described in the Concept Paper avoids inventorying all cyber assets by defining BES Reliability Functions and BES Subsystems first and using those to screen cyber systems; however, FMPA believes that the methodology, as laid out, does not cause entities to avoid a complete inventory of cyber systems that touch the BES (e.g., it would eliminate systems like billing systems, for instance, but, it does not eliminate relays, RTUs, and other cyber systems used for BES purposes). Also, the industry has faced criticism that we may have overlooked cyber systems and their interactions. Hence, FMPA believes that we will likely need to inventory all of our cyber systems that touch the BES anyway, so why have two intermediate steps of defining BES Reliability Functions and BES Subsystems, why not proceed directly to an inventory of cyber assets that touch the BES and a threat analysis of those cyber systems? Rather than creating a new definition of BES subsystems, the risk-based methodology for determining critical cyber assets might be better served in categorizing types of threats that can cause "instability, uncontrolled separation, and cascading outages", e.g., 1) sudden loss of supply, 2) sudden loss of demand, 3) threat of thermal cascading (e.g., loss of one facility causing an overload on another facility causing that facility to trip, then overloading another facility causing that facility to trip, etc.) and any resultant mismatch of supply and demand, 4) threat of voltage collapse and the resultant mismatch of supply and demand, etc. FMPA is aware of some people's concern of malicious use of lower impact cyber systems (e.g., a relay or RTU) to access

Question 1

	more critical cyber systems such as Energy Management Systems, using the lower impact cyber systems as "gateways". However, it makes more sense to regulate the fortification of the Energy Management System from such malicious use than to regulate fortification of every digital relay. As an analogy, the electronic banking system is another one of society's vital infrastructures. For such as system, it makes sense to regulate cyber security of central banking systems that, if maliciously used, could dramatically impact our economy. It does not make sense to regulate cyber security on personal computers individuals use to perform on-line banking. It is important to understand that the intention of the standards is NOT to regulate every aspect of an entity's business, but only those aspects that can cause "instability, uncontrolled separation, and cascading outages". Just because the standards may not apply to non-critical cyber systems does not mean that entities will not have cyber security measures for those cyber systems. We are simply expressing that there is no need to regulate the security measures on those non-critical systems.
SWPA	Yes, the concept is clear. But why do we need another approach? There has not been sufficient time for the industry to judge the effectiveness of the current Critical Asset/Critical Cyber Asset approach. Give this a chance. If the issue is with entities that are dodging the process by creating a methodology that guarantees them to have no Critical Assets, then address that problem before you throw it all out. In other words, define what equipment/systems are critical cyber assets. Perhaps a hybrid of both is the best approach? Regardless of whether you use the "reliability functions" approach or the "Critical Cyber Asset" approach, the scope of the CIP Standards should be limited to systems that could cause instability, uncontrolled separation, or cascading failures on the BES as a result of a cyber security incident. In Section 215 of the 2005 Federal Power Act there is a definition for "reliability standards". This definition does not direct the ERO to apply burdensome standards to all facilities or systems owned or operated by a registered entity regardless of impact. It is not reasonable to require entities to be responsible for monitoring compliance on facilities and systems that have little or no impact to the BES. This will force entities to divert a large amount of resources away from system improvements or disconnect communication lines or both. It is our opinion that the results of this proposed change will ultimately decrease BES reliability and further burden the limited resources that NERC has for monitoring compliance to standards that are proven to enhance BES reliability.
CPE	While the concept may be clear, CenterPoint Energy disagrees with the concept and believes it unnecessary and premature to so completely alter this fundamental step before CIP-002 is implemented by a majority of responsible entities. Much time and effort has been expended trying to understand and implement the current requirements. Indeed, Table 2 entities are already required to be compliant with CIP-002 and Table 3 entities are well on their way. To suggest a radically different approach at this stage is, at best problematic and at worst, may cause some entities to rethink their positions and possibly miss the implementation date and therefore risk non-compliance. The suggested approach of viewing the BES holistically and identifying BES functions is overly broad and not needed. Most entities do not have the capability needed to view the BES holistically. Identifying assets that are critical to the reliable operation of the BES and those cyber systems that are essential to the operation of those assets is a much more concrete

Question 1

	approach and, CenterPoint Energy believes, renders results that are at least comparable and possibly better than the suggested approach. Market functions should not be considered as critical to the reliability of the BES. It is common for emergency procedures to include the suspension of certain market activities until the emergency condition is resolved and yet the essential BES operations continue. This suggests that market functions are not critical to the reliability of the BES. Including distribution feeders as a BES Subsystem is another issue with which CenterPoint Energy disagrees with the SDT. In a blackstart restoration process, it becomes necessary to add load to stabilize the system. However, there are many options when it comes to which distribution feeder to use therefore, criticality of individual feeders to the restoration process is lessened. The inclusion of distribution feeders using a "function based" approach illustrates the pitfalls of such an approach. An asset based approach enables consideration of the diversity of assets to perform reliability functions. CenterPoint Energy believes the current process of identifying Critical Assets and then the Cyber Assets essential to the operation of the Critical Assets is a reasonable approach. CenterPoint Energy believes it is the best interests of all parties to allow the full implementation of the current CIP-002 Standard. As with any other Standard, compliance audits and spot checks may reveal additional issues for future consideration.
GTC	GTC agrees that this concept is clear in that it ties the categorization to the reliability of the Bulk Electric System, which is the goal of NERC standards in general. It is unclear, however, how this categorization takes place for a subsystem owned by a single entity where the subsystem performs functions of the BES for multiple entities (i.e. a substation RTU that is performing Control and Operation for one entity, performing situational awareness for another, and System Stability for yet another entity.)
DYONYX	First, the industry has spent hundreds of millions of dollars addressing the concept of Critical Assets and Critical Cyber Assets, reconfiguring network architectures to minimize exposure, and designing appropriate compliant security programs with an array of physical and cyber security protective measures. Now we are proposing a completely different paradigm to identify Critical Assets, hence forth to be defined as "BES Subsystems", with an astonishing level of detail that may well supersede a large component of the effort made to date. The point is that the particular categorization of systems by functions methodology proposed herein is way too complex and therefore hard to understand. In review of Sections I, J, and K, it is totally overkill, very time consuming, and in our opinion, unsustainable. While protecting these infrastructures is extremely important, we believe some degree of prudency and consideration for workability and sustainability should be taken? Having said this, we believe the concept of categorization of cyber systems by their impact on the reliability "functions" is conceptually a very logical approach. The drafting committee is to be commended for their effort. However, from a practical perspective, by starting with a "generalized" definition of reliability, e.g., the ALR definition, the number of "BES Functions" and ultimately "BES Subsystems" and "BES Cyber Systems" for analysis will increase significantly. The ALR may be appropriate for other "operating" standards, but does not appear to be appropriate for identifying Critical Assets / BES Subsystems. There

	are too many subjective terms in the ALR definition and accordingly the translation to the example set of defined "functions" appear to be prescribed. For example, the sixth characteristic defined under the ALR definition states; "The Bulk Electric System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components." What exactly does this have to do with the need to apply a high level of security to specific assets when the real problem is in the inadequacy of the design of the BES itself, i.e., insufficient generation capabilities, etc.? While the proposed approach appears to be designed to facilitate a means to establish various "levels" of criticality, is it really necessary to identify and categorize the systems at this level of detail? Do "Low", "Medium", and "High" attributes tell us anything relevant about the different measures that should be applied to BES Cyber Systems? We believe the two categories of "Critical" or "Not Critical" are indeed adequate. The current CIP Reliability Standard CIP-002 specifies that Critical Assets may be facilities, "systems" or equipment. We believe the current approach, with appropriate recognition of the impact "systems" can have on the reliability of the BES infrastructures and specific enhancements (many of which were identified in the Guideline), is a more feasible, less complex, and workable approach. In this regard, "Systems" are defined as Critical Assets themselves if, when compromised or otherwise removed from service, can impact the reliability of the BES. A "System" can impact the reliability of the BES if they impact other Critical Assets or "Non-Critical Assets together of which" impacts the reliability of the BES, e.g., an "EMS "system" that controls a large array of substations, neither of which is a Critical Asset, but "together" impacts the reliability of the BES, will be deemed a Critical Asset. This approach also eliminates the confusion about "control room" and "control centers"; it is the impact that the underlying "systems" within the control room or control center have on the reliability of the BES that is important, which has nothing to do with the definition of the "facility". See comment in Question # 5. With this approach, "reliability" of the BES from a Critical Asset perspective needs to be more precisely defined rather that the broad definition of ALR as proposed. Recommendation: Keeping in mind the concept of "common mode failures" as discussed in the "Security Guideline for the Electricity Sector: Identifying Critical Assets" and the analysis of systems as discussed above, we believe an extension of the existing CIP-002 R1 / R2 Standards utilizing the asset-based perspective builds on existing operational thinking, is less confusing, and will certainly be less onerous to administer and implement. The conceived functional approach, coupled with the proposed level of detailed, will generate hundreds of controversies, endless topics of subjectivity, and literary millions of hours of analysis. Adding in third party dependency analysis provisions amplify our concerns. In summary, the categorization of systems approach, while theoretically logical, is too cumbersome and complex. It has not worked well in the federal space.
BPA	Yes – "but the implications are not clear." – Over arching all the standards?

Question 1

	– A Lot of work – same results. The indication was non-inclusive regarding the examples and the BES Function relationships. If non-inclusive, does that mean entities have the ability to exclude a Subsystem or Cyber System?
EEI	On behalf of its member companies, EEI appreciates the opportunity to provide comments on the ***Categorizing Cyber Systems — An Approach Based on BES Reliability Functions*** **concept paper** developed by members of the Drafting Team. 1) EEI recognizes that: a. In Order No. 706, the Commission determined the CIP standards to be Mandatory and Enforceable. In that Order, the Commission also: i. Determined that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. (Order No. 706 at P 253.) ii. Believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. (Order No. 706 at P 25.) b. Congress has voiced concern regarding appropriate protection of critical infrastructure, including recent hearings and draft legislation discussions in the: i. Senate Committee on Energy and Natural Resources, ii. The House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. 2) EEI agrees that the appropriate identification and protection of Bulk Electric System (BES) critical assets and critical cyber assets are vital to the interests of the electric consumers and the nation. Asset owners recognize their commitment and obligation to protect cyber assets and cyber asset subsystems that are essential to the reliability of the BES. 3) EEI believes that the introduction of the concept paper represents a significant development for the protection of the BES. a. The concept paper identifies the opportunity to consider the evaluation of cyber assets and cyber systems that may impact the reliability of the BES but may not be directly connected to or associated with a single critical asset, such as a particular transmission substation or specific control center. b. The concept paper correctly identifies: *A crucial undertaking for the drafting team lies in developing these security controls in such a way as to* mitigate *risk while maximizing the value of the associated cyber security investment for the industry. To accomplish this objective, the drafting team seeks to develop a library of controls (requirements) appropriate to the degree and type of protection needed.* (concept paper, page 3, line 36)

	c. The concept paper identifies potential dependencies of elements of the BES upon cyber systems that may not be initially obvious. 4) EEI recommends the following improvements for the concept paper, and subsequent standard draft language: a. Elements to add to the concept paper: i. Additional language regarding risk assessment, including consideration of probability, or likelihood of adverse acts against critical cyber assets. ii. Definition of threat basis. In order to appropriately assess potential threats, including impact assessment, and subsequent mitigation strategies it is imperative that the threat be defined. Failure to define the threat can result in misallocation of resources that may leave the BES unprotected. iii. Given the current negative financial climate that our customers, companies, and regulatory agencies are operating within, it is important for mitigation methods to focus on reducing the greatest amount of risk for the least cost. iv. It may be appropriate for the concept paper to identify that certain cyber systems simply do not affect the reliable operation of the BES. v. Identification of potential contingencies that need to be considered in light of electromagnetic pulse (EMP) or geomagnetically induced current (GIC) events b. Elements to modify or eliminate from the concept paper: i. Care should be taken to avoid identification of functions that are inconsistent with the NERC Functional Model, or established utility practice. ii. The use of over-broad functions that may have elements with differing risks or impacts should be avoided, as this may lead to confusion and/or inappropriate (ineffective) security control identification. As an example from the concept paper itself: *Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. For example, a control system in a small generating facility may have a different reliability impact on the BES than an identical control system operating a larger or several generating facilities.* (concept paper, page 15 line 27) 5) We believe that the interest of protecting the reliability of the BES would be best served through the application of the following principles: a. The industry has made a significant investment and concerted effort toward protecting critical assets and critical cyber assets under the original identification framework. We recommend that the valuable elements of the new approach be used to augment or enhance the legacy identification framework, rather than face the risk of loss of

Question 1

	momentum and forward progress while the industry wrestles to understand and incorporate an entirely new methodology. b. An example of positive forward progress using the legacy identification framework, is the development of new guidelines for identifying critical assets and critical cyber assets. The opportunity is to build on the existing identification framework. c. The focus on identifying cyber assets or subsystems deserving of extra protection should be tied directly to a role that is *essential* for the reliable operation of the BES. We are concerned that the concept paper may call for a disproportionate level of protection for a vast number of cyber assets. d. Language developed within the concept paper or subsequent standards should be written in a way to be able to retire/reduce the need for Technical Feasibility exceptions (TFEs). e. Language developed within the concept paper or subsequent standards should provide for methods of identification of criticality and due process in the event of disagreements over designation. f. Careful consideration should be given to the discussion of multi-layer criticality matrix identification methods. The industry may be better served with a simpler method of designation and identification. g. The requirements for documenting the determination of criticality should be designed to minimize unnecessary administrative overhead. h. We suggest that the drafting team focus on the "What" of security control outcomes rather than the "How". i. We suggest that the drafting carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
SDGE	Yes, the concept of categorizing by function is clear. It helps to provide a "Big-picture" viewpoint to the categorization process instead of starting by selecting assets.
GSOC	The concept as a whole is headed in a way to achieve better consistency in categorizing assets. This section is brief and could easily lead to confusion.
BGE	• Parts are abstract, hard to understand, and will sometimes demand a large amount of documented analysis to reach an obvious conclusion. It for example contains an example that a relay may be a relevant (in-scope) cyber system because it supports a transmission line (a BES subsystem), and the loss of the line may result in the impairment of the ability to manage loading constraints (A BES reliability function). The sheer burden of documenting and evaluating the one to many relationship between any relay or set of relays and a less than definitive catalog of BES reliability functions

Question 1

	compares unfavorably with the simpler approach that we use under the current standard (A relay in a "critical asset" station is in scope). Not sure that avoiding one-size-fits-all security measures is an economical trade off; it seems properly scaled security could have been approached in a simpler way such as defining different levels of criticality for critical stations based on established contingencies (including the successful hack of a discrete ESP) and transmission planning criteria. • In general, this is a dramatic change in philosophy that will take some time and resources to accomplish the change. There should be a clear time frame for implementation that is possible to meet. • Section C is implying that any system which does the function listed in table 1 can be considered as BES Cyber System. Based on Table 1 Load Management Section, any system providing Demand Response and Smart Grid functions will be a Cyber System affecting BES. However, in the Figure 5, AMI System is shown as just a Collateral System. Does this mean AMI System by itself is not a Critical Cyber System? Elaborating Section C and Table 1 by providing specific examples around AMI and Demand Response System will be very helpful.
CUSMO	Yes, the concept is clear. But why do we need another approach? There has not been sufficient time for the industry to judge the effectiveness of the current Critical Asset/Critical Cyber Asset approach. Give this a chance. If the issue is with entities that are dodging the process by creating a methodology that guarantees them to have no Critical Assets, then address that problem before you throw it all out. In other words, define what equipment/systems are critical cyber assets. Perhaps a hybrid of both is the best approach? Regardless of whether you use the "reliability functions" approach or the "Critical Cyber Asset" approach, the scope of the CIP Standards should be limited to systems that could cause instability, uncontrolled separation, or cascading failures on the BES as a result of a cyber security incident. In Section 215 of the 2005 Federal Power Act there is a definition for "reliability standards". This definition does not direct the ERO to apply burdensome standards to all facilities or systems owned or operated by a registered entity regardless of impact. It is not reasonable to require entities to be responsible for monitoring compliance on facilities and systems that have little or no impact to the BES. This will force entities to divert a large amount of resources away from system improvements or disconnect communication lines or both. It is our opinion that the results of this proposed change will ultimately decrease BES reliability and further burden the limited resources that NERC has for monitoring compliance to standards that are proven to enhance BES reliability.
MH	The concept to categorize based on reliability functions is clear. Using NERC's definition of Adequate Level of Reliability (ALR) as foundation to categorize cyber assets is a good idea. If the revised CIP Standards require Responsible Entities to use this approach for their individual assessment then the terms "reliability function" and "BES subsystem" should be added to the NERC Glossary of Terms. The list of reliability functions should be vetted within NERC by the Operating and Planning Committees in addition to the project team. The concept to categorize based on reliability function could be used by the project team to develop a prescriptive table for use

Question 1

	within the CIP Standards. The Responsible Entities could then use the table to categorize each of their BES subsystems. In this scenario, the reliability function definition and detailed description might not be necessary as part of the CIP standard.
NST	We believe the explanations in Section C and related sections are adequately clear.
NPCC	Agree on the concept but have implementation concerns.
RFC	Yes
IRC	Yes—the new concept and paradigm for categorization by BES Functions are clear. The external third-party review requirements of FERC Order 706 (section 322) were not addressed in this paper. FERC Order 706 stated that "an external review of critical assets by an appropriate organization is needed to assure that such lists are considered from a wide-area view (i.e., from a regional perspective) and to identify trends in critical asset identification." FERC indicated in Order 706 that allowing external review as a voluntary measure would not be adequate. While many Registered Entities want the RCs to perform this function for them, the use of RCs to perform the oversight role is problematic since 12 of the 17 current RCs are also registered to perform functions such as BA, TOP, IA, etc. How can an ISO RC conduct an external review of the same ISO BA functions? The SWG reiterates that we do not believe that RCs/BAs (that do not own the bulk electric system assets (e.g., generation/transmission) should play a functional role in identifying or providing oversight of "cyber assets" among such asset owning companies.
FE	The concept is fairly clear but the approach is too complex and over-reaching in the number of cyber systems that can practically be implemented and implies that all cyber systems have some level of BES impact. The industry should not significantly deviate from the process of first identifying Critical Assets and then the Critical Cyber Assets but rather aim to refine, improve and achieve a more consistent Critical Asset determination across industry. FE believes the appropriate path forward is to continue to focus on the guideline documents developed by the Security Guidelines Working Group (SGWG) for the currently effective version of CIP standards. The guidelines for Identifying Critical Assets and Critical Cyber Assets should be the basis for what forms the next generation of mandatory and enforceable reliability requirements for the CIP-002 standard. The industry has made a significant investment and concerted effort toward protecting Critical Assets and Critical Cyber Assets

Question 1

	under the current identification framework, and it is on the eve of full implementation after 3 years of development. To take such a dramatic and complicated departure from the current path with the proposed concept would undermine progress and impede momentum. It is not evident that the proposed approach would provide a significant improvement in reliability over the existing approach or that any marginal benefit would be cost-effective given the labor intensive process outlined by the concept paper. While some elements of the new approach may be used to augment or enhance the current identification framework, FE recommends working from the current framework rather than the proposed concept going forward. Therefore, the team should consider a hybrid approach that simplifies and improves the Critical Asset determination by requiring a certain class of facilities such as Extra-High Voltage (EHV) that form the backbone of the BES classified as Critical Assets and thereby requiring a detailed inventory and assessment of any cyber assets related to their reliability function. Such an approach can improve reliability by cost-effectively protecting a broader set of BES assets. Regardless, the final approach taken should ultimately recognize that not all cyber assets should require enforceable regulatory oversight and that only the most essential functions or class of facilities should be covered.
AEP	AEP appreciates the drafting team posting the concept paper for review and allowing the industry the opportunity to comment. The approach outlined in the concept paper is challenging to understand as a result of the proposed paradigm shift. Moreover, this concept paper introduces numerous new concepts/terms and uses many interrelated terms, which could result in the terminology being convoluted. While the proposed methodology is less ambiguous than the current methodology, this concept paper is a potentially significant expansion of project scope without a commensurate reduction of risk. In addition, this framework makes the process very complex, which does not necessarily advance the intended objective of improving security and reliability. In general, more complex requirements may result in less security and reliability of the BES. The requirements of the current NERC CIP standards provide an adequate technical/regulatory framework to achieve the desired security improvements, as well as the basis for enforcement actions to address identified noncompliance. We suggest that the industry builds upon the framework that has been developed in versions 1 and 2 of the CIP cyber security standards through a set of structured interim progression of steps. It appears there are some concerns around the implementation of version 2 of CIP-002. We support modifications to address those concerns, with the exception of implementing a significant paradigm shift and a complete do-over without giving any recognition to what has already been done. AEP believes the concept of categorizing by function instead of by asset significantly broadens the scope and complexities without any significant benefits and without giving due consideration to what already has been done. The present methodology, which is based on the concept of asset protection, is well known and understood by the industry. Moreover, not all elements within a broad categorization by function are equal, nor have equal potential impact, if any, to the BES. We strongly urge the Drafting Team to reconsider the function-based concept. We recommend the Drafting Team continue with what has been implemented and enhance the current asset based system, as required.

Question 1

MGE	The proposed idea of "functions" is one possible way of identifying BES Subsystems that affect the reliability of the BES. Disagrees with the term of "operability" within the first sentence of section C. Unless it is used as it is defined by section 215 of the Federal Power Act: The term `reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements. If the term is not used as described, this could lead to an interpretation that all assets will be categorized as BES Subsystems. The SDT used a yet to be defined term "Reliability Functions" (and BES Function). This question cannot be totally answered until 1, Reliability Function is defined or 2, a supporting document is presented as to what the basis is of the defined Reliability Function. As written within this Concept Paper, "Situational Awareness" is given as an example. This should be removed from the applicability except for RC, TOP, and BAs, due to it is redundant to Control and Operations, the SCADA or EMS is designed to give the entity awareness of their system and status states, this will give others entities the ability to perform situational awareness of their system.
WE	While the concept is clear, Wisconsin Electric does not support changing the current risk based assessment to determine critical bulk electric system assets and associated critical cyber assets. If there's concern over uniform application of a risk based methodology by responsible entities, then we recommend further refinement of the current process to perform the risk analysis. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	The broad concept is fairly clear, but the details are not well articulated, and the approach may be too complex for the industry to embrace. We do not believe the methodology should proceed from the Adequate Level of Reliability as it is defined here. The sixth characteristic, supplying load at all times, would inappropriately expand the scope of the cyber security standards to distribution assets and systems. Supplying load is a service reliability issue as opposed to a BES reliability issue. The Introduction section implies a vastly expanded scope for the standard development in using terminology such as "at all times" and "identify all cyber systems". Order 706 required a risk based methodology. Risk is a measure of both consequences and probability – this methodology is based solely on consequences while ignoring probability of failure, which accounts for part of the vast scope increase. The concept would also be clearer if it was stated exactly what the cyber security standards are trying to protect against – is it intrusion and subsequent disabling of centralized control systems that would results in collapse of the BES, or is it physical or cyber damage to discreet transmission assets that could cause cascading failure, or both? In order to facilitate a common understanding, definitions should be provided for the BES Functions.
SOCO	Yes, the concept is clear.
E-ON	Yes. The BES function of assets is an integral part of the risk-based methodology currently employed to determine whether an asset is critical to BES reliability. However, while the concept is straightforward the manner in which the Concept Paper

Question 1

	proposes to implement the concept is very disconcerting. The BES characteristics that are intended to inform the identification of BES Reliability functions go beyond what is required to maintain BES reliability
ATC	The concept paper does not provide enough details associated with categorization of functions to answer this question. The existing concept of critical asset identifies the type of event a company needs to consider (Cyber related attack), and a list of assets that need to be studied and the level of protection required for critical cyber assets. The concept paper does not address the questions of the type and severity of incident we are expected to protect against and the associated level of protection. This paper needs to provide more detail as to why the proposed concept is an improvement over the existing system, how it will improve reliability, the compliance obligations (Cyber and Physical security) associated with these changes, and how the transition from the existing CIP-002 Critical Asset identification regime to the categorization approach will occur.
OMPA	OMPA understands that the concept paper is proposing a paradigm shift from identifying or categorizing cyber resources from equipment or assets to a process or systems approach. However, the application of using a methodology to identify all cyber systems which support the reliable operation of the BES based on NERC's definition of Adequate Level of Reliability (ALR) is still unclear. This appears to be an extensive and tedious process to flush out for an entity that does not currently own or operate critical assets. Can we assume "BES" is still based on the definition in NERC's Statement of Compliance Registry Criteria (v 5.0)? It is also unclear if, or how, this methodology will align or be incorporated with the actual standard and if, or how, this process/methodology will be monitored/audited.
TAPS	As an informal association of TDUs dependent on the grid, TAPS believes NERC is on the right track in focusing not on individual BES and cyber assets, but on the interaction of BES assets in identifying which cyber systems must be protected from cyber attacks. For our nation to cost-effectively protect the grid from the types of cyber attacks that Congress cared about in enacting Section 215—those that would threaten instability, uncontrolled separation, and cascading outages—the identification of cyber assets requiring protection needs to focus on the cyber systems supporting BES assets that could create those wide-scale outages. When we bank online, it is up to the bank to protect its systems from any virus that may have infected our home computers. In the same way, what is key for purposes of Section 215 cyber standards is protecting from cyber attack the cyber systems that matter, e.g., those cyber systems that could compromise the reliability of the BES, rather than putting armor on every computer that interfaces with such cyber systems or otherwise makes any contribution to keeping the lights on anywhere. While we respect the aim of the SDT, it went off course when it defined BES Reliability Functions for purposes of cyber security based on Adequate Level of Reliability. Use of the ALR criterion to define BES Reliability Functions and BES Subsystems would sweep in virtually all BES facilities, and the cyber systems that support them as BES Cyber Systems meriting some level of protection. As shown on page 4 of the Concept Paper, ALR includes "the ability to supply the aggregate

	electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components." The Concept Paper concludes, at page 4, "These BES subsystems may be defined as facilities, equipment, or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability." Using the ALR construct as a guide, virtually all BES functions and facilities would be included in BES subsystems because, almost by definition, they have been planned to serve load during some time frames taking account of scheduled and expected unscheduled outages. Such inclusion would lead to inappropriately gold-plated cyber security requirements that do not advance Section 215's statutory objective – avoiding instability, uncontrolled separation, and cascading outages. Rather, the focus of categorization of cyber facilities that warrant protection by NERC cyber security standards should be guided by the statutory definition of "reliable operations" that reliability standards are intended to achieve: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." FPA Section 215(a)(4). *See also* Order 706 P 234 & n.79, quoting the "reliable operations" definition as giving meaning to NERC's definition of "critical assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Incorporating the statutory "security-focused" criterion for assessing BES reliability functions and subsystems (in lieu of the Concept Paper's ALR criterion) would result in a more appropriate subset of the facilities and cyber systems that make a difference in terms of avoiding instability, uncontrolled separation, and cascading outages, and which therefore merit protection from cyber attacks. Such a focus would also more appropriately target our cyber protection efforts (and resources) at protecting the assets that matter, rather than needlessly burdening the economy with expenditures to secure facilities that do not matter from a security perspective. Further, while we appreciate that the SDT circulated the Concept Paper before all the concepts have been fine-tuned, TAPS is concerned about how these concepts can be developed to produce clear and auditable standards that registered entities can apply with confidence as to their compliance and that do not unduly burden Regional Entities from an enforcement point of view. The determination and mapping of BES Functions beyond those identified in the Functional Model, and identification of BES subsystems by (as yet undisclosed) "predefined criteria" may be needlessly complicating steps. It might be clearer and more direct to require each registered entity to inventory and evaluate each of its cyber assets to determine whether they have an impact on BES facilities that are critical to system security — avoiding instability, uncontrolled separation, and cascading outages. Consistent with Order 706's directive, as reflected in Order 706-A at PP 30, 33-34, that NERC provide "relatively smaller" entities with guidance and technical support in determining whether their assets are critical to the reliability of the Bulk Power System (thus presupposing that some assets will *not* be critical), the focus should remain on "critical assets," not all BES assets.
GWA	Yes.

Question 1

MISO	Categorizing the functions into high, medium, and low categories is a significant paradigm shift from the current set of CIP standards. The drafting team appears to be operating with the assumption that this paradigm shift is appropriate and they just need the industry to weigh in on how to make the categorization effort better. The drafting team needs to determine if industry is agreeable to switching from the existing critical and non-critical approach to the high, medium and low impact categorization.
SCEG	Yes
GEEI	The concept of categorizing by function instead of by asset is clear, but there will be functional overlap in practical application. Examples of functions and their classification would be help to clarify.
LES	No. LES is in agreement with the comments submitted by the TAPS organization and additionally, LES believes the intent of the current version of standard CIP-002 has a better security focus than the proposed concept paper, and that the current version of standard CIP-002 should be maintained. The current version of standard CIP-002 identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. It then goes one step further by differentiating between routable and non-routable connections to these cyber systems, since non-routable connections are inherently more secure against, and limit potential damage from, remote attacks. This appears to be a straight forward and direct approach to securing the BES from cyber attack, and LES does not see any reason to deviate from this approach. If the concern is too much latitude in the current version of standard CIP-002, then maybe the new risk assessment guidelines should be officially amended to the current standard, assuring that all entities identify critical assets under a similar, Engineering study based assessment. Replacing the existing standard with an entirely new approach does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security.
MRO	No, the proposed process in the whitepaper does not provide any additional clarity or value versus the current process that is currently in place in CIP-002. It appears that the categorization approach would replace CIP-002 Requirement 1. Section C does not appropriately apply the Adequate Level Of Reliability as listed in Section B. The MRO NSRS believes the intent of the current version of CIP-002 standard has a better security focus than the proposed concept paper and that the current version of CIP-002 standard should be maintained since this concept paper does not elaborate in Section A on the maximum value the industry will receive by switching to this next risk-based assessment methodology plus, in Section C of this concept paper, an impact assessment is mentioned but it was not described how this assessment will be accomplished. The current version of CIP-002 standard identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. This appears to be a straight forward and direct approach to securing the BES from cyber attack and MRO NSRS does not see any

Question 1

	reason to deviate from this approach. If the concern is too much latitude in the current version of the CIP-002 standard, then maybe the new risk assessment guidelines should be officially amended to the current standard, assuring that all entities identify critical assets under a similar engineering study based assessment. Replacing the existing standard with an entirely new approach does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security.
MEC	No, the concept of categorizing by function is not clear. MidAmerican recommends retaining the designation of which BES physical assets are Critical Assets as the first step in the process of selecting Cyber Assets to protect. This clearly sets priorities to ultimately ensure that the most BES consequential assets have been protected. CIP-002 can be improved to achieve more consistency within the industry without abandoning the concept of Critical Assets. Specifically, descriptions for three of the seven asset categories that shall be considered in CIP-002 R1.2 include more detail descriptive criteria than the other four that generically refer to "support the reliable operation of the Bulk Electric System." Replace this generic phrase in those four sub-requirements with suggested criteria that corresponds to and complements existing industry requirements that are already defined for BES operations. This proposed change is more direct, achievable and clear than functional categorization. MidAmerican is concerned with the impact categorizing by function may have on the remaining CIP standards, as well as possible further delays and more confusion in an already complicated process. In development of the list of Critical Assets, it is then essential to comprehend what type of threat the BES is facing. Cyber threats are different than traditional threats to the reliability of the system. When protecting against cyber threats invoked by a malicious entity each responsible entity must assume that all of its BES facilities are under attack simultaneously. The responsible entity needs to determine which of these facilities (control centers, substations, generating plants, etc.) is critical to the BES and ultimately which Cyber Assets or systems support these critical facilities. Security controls are then selected to materially lower the probability and/or impact of a significant event for a specific type of Cyber Asset (for example, a relay verses a Windows PC). MidAmerican's recommended approach leverages both NERC's functional model and NIST together to benefit the cyber security of the BES. The core competencies of the NERC functional model are leveraged in selection of the Critical Assets. NIST's security controls core competencies are then leveraged in protection of the Critical Cyber Assets essential to the Critical Assets. Additionally, this approach leverages risk management guidance from the International Organization for Standardization (ISO), a worldwide federation of national standards bodies. ISO/IEC Guide 51 provides a basic risk vocabulary to develop common understanding. This guide simply defines risk as the combination of probability of an event and its consequence. Consequences (impacts) are addressed throughout the concept paper. Probability has a material role in risk management, but is not fully developed in the concept paper.

Question 1

PSEG	PSEG supports the basic philosophy that future revisions should focus on the systems that protect the BES based on their significance to maintaining Adequate Level of Reliability, rather than their connection to a Critical Asset. However, the drafters need to be careful to ensure the work entities already have in place for CIP 002 Versions 1 and 2 compliance does not conflict with the Version 3 standard.
SCE	**GENERAL COMMENTS OF THE SOUTHERN CALIFORNIA EDISON COMPANY** Southern California Edison ("SCE") appreciates the opportunity to submit comments in response to the North American Electric Reliability Corporation's ("NERC") July 2009 concept paper titled "Categorizing Cyber Systems - An Approach Based on BES Reliability Functions" ("Concept Paper"). SCE understands that NERC drafted the Concept Paper in response to Order 706 issued by the Federal Regulatory Energy Commission ("FERC"). SCE continues to study the Concept Paper and reserves the right to supplement its comments as more information comes to light. However, assuming that the industry moves from the current risk-based approach to cyber security to the impact-based approach discussed in the Concept Paper, SCE makes the following comments intended to best ensure the reliability of the Bulk Electric System: First, the wholesale shift in direction proposed in the Concept Paper for Version 3 of CIP-002 would be so massive and revolutionary in scope that any changes to CIP-002 would affect its sister standards. For example, the Concept Paper notes that the shift to an impact-based system would require a new "library of controls" that would differ from asset to asset based on "the degree and type of protection needed." [Concept Paper, at pg. 30, lines 17-20]. Such controls would likely replace standards CIP-003 through CIP-009, which are calibrated to the current risk-based approach to cyber security. Therefore, in order to fully understand the potential impact of this new system, SCE urges NERC to present its proposed library of controls concurrent with version 3 of CIP-002. The common goal is to enhance the reliability of the Bulk Electric System. In order for the energy industry to determine whether the proposed revisions would accomplish that goal, the industry needs enough facts to make a reasoned analysis. Next, designing the proposed revisions will require careful thought and planning. As noted by the Concept Paper, the proposed move to an impact-based approach to cyber security represents nothing less than an industry-wide "paradigm shift." [*E.g.,* Concept Paper, at pg. 3, lines 44-45]. Simply "fast-tracking" the complex ideas presented in the Concept Paper would not necessarily enhance the protection of the bulk electric system. Instead, such an approach could lead to confusion and uncertainty as it would force the energy industry to grapple with hurriedly, and thus potentially poorly, drafted standards. Designing a paradigm shift for an entire industry requires a calm and deliberative development period with significant stakeholder and expert input. [*E.g.,* Concept Paper, at pg. 3, lines 50-51; pg. 8, lines 34-36; pg. 30, lines 31-32 (discussing opportunities for industry input)]. Finally, assuming that NERC's proposed revisions are adopted, SCE urges NERC consider a "phased in" approach to implementing this paradigm shift. By definition a paradigm shift is something that cannot be easily and quickly implemented. The energy industry will likely need time to acquire the technical, human and financial resources necessary to study, understand, and implement the impact-based system. A phased-in approach that implements this new paradigm shift in

Question 1

	discrete, measured, chunks would likely enhance the reliability of the Bulk Electric System more effectively than by introducing this new system in one single installment. SCE also agrees with, and joins in, the following sections of the comments submitted by the Edison Electric Institute on this matter: Section 4(a)(i)-(iv); Section 4(b); Section 5(c) – (g).
AWEA	The concept is clear but the implementation is not. It is relatively easy to make a list of physical assets that is exhaustive and mutually exclusive (generators, substations, …) thus covering the entire system while also avoiding double counting. "BES Reliability Functions", on the other hand, can be defined in many ways. One example of a specific concern involves the categorization of variable energy resources such as wind plants and other renewable resources. They are predominantly energy suppliers with limited, but non-zero, capacity value. They are not peaking units or contingency reserve providers. They are not balancing resources. They may or may not impact frequency. Defining a robust system of BES Reliability Functions that is exhaustive and mutually exclusive may take more time than is available if a standard is to be posted for comment in 2009.
APPA	As an an initial matter, I agree with the SDT's general approach and I agree it is a paradigm shift. However, I find it difficult to envision how the industry will apply it in practice while ensuring effective compliance. The concept of categorizing BES Subsystems and Cyber Systems based on reliability functions to develop Cyber System Targets for Protection with different levels of protection based on the importance of the system makes a lot of intuitive and common sense. It responds to the common-mode failure risk associated with cyber systems associated with multiple BES systems. It responds to the fundamental problem that CIP-002 now presents – that once an asset is categorized as critical, an extreme level of cyber protection may be imposed under CIP-003 through CIP-009 – while no protection is required for assets that are not classified as critical. Nonetheless, I have major concerns that the SDT's conceptual approach will be extremely difficult to implement, particularly since the categorization proposal does not appear to be tied directly to NERC's other reliability standards. Developing an industry consensus around a set of BES Functions such as those shown in Table 1 would appear to be a precondition for implementing this approach. Developing that industry consensus in support of a well-defined set of BES functions, BES Subsystem Criteria, and a comprehensive identification of well-defined BES Subsystems and Cyber Systems within the industry is likely to be exceedingly difficult. Further the BES Functions and BES Subsystems (Facilities, Equipment and Cyber Systems) shown in Figure 1 overlap. The SDT could approach this task based on the NERC Functional Model – but that model is just that - a model of functional activities that does not consistently describe how specific registered entities have organized their operations. Each registered entity could attempt to develop its own functional analysis of operations and its associated BES systems and Cyber systems, but under that approach consistent application across entities is likely to be problematic and enforcement is likely to be burdensome, unless there are clear categorizations of facilities, e.g., all BA and TOP control centers that serve more than x

Question 1

	MW fall in one risk bucket, while smaller control centers fall into a lower risk (and thus lower mitigation tier) bucket. Also, the reliance on Adequate Level of Reliability (page 4, lines 28-45) may be problematic, particularly the last definition, point 6. ("The Bulk Electric System has the ability to supply the aggregate electric power and energy requirements of the electric consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.") In the current context, this sub-criterion could be read to require all BES systems and cyber-systems to be identified as critical and thus requiring CIP protection since we are not in the business of building facilities that are not needed for the "reliability or operability of the system" (page 4, line 9).
PAC	No, the concept of categorizing by function is not clear. PacifiCorp recommends retaining the designation of which BES physical assets are Critical Assets as the first step in the process of selecting Cyber Assets to protect. The current approach of identifying critical assets ensures that the most consequential assets to the BES have been protected. This has become an accepted approached used by the industry as well as several Regional Organizations. The currently approved standards can be improved without abandoning the concept of Critical Assets. The concept paper defines several BES functions that were not specifically addressed in the evaluation criteria described in previous guidance documents of currently approved standards. PacifiCorp recommends adding these BES functions to the standard's language. In development of the list of Critical Assets, it is essential to comprehend what type of threat the BES is facing. Cyber threats are different than traditional threats to the reliability of the system. When protecting against cyber threats invoked by a malicious entity each responsible entity must assume that all of its BES facilities are under attack simultaneously. The responsible entity needs to determine which of these facilities (control centers, substations, generating plants, etc.) is critical to the BES and ultimately which Cyber Assets or systems support these critical facilities. Security controls are then selected that materially lower the probability and/or impact of a significant event for a specific type of Cyber Asset (example, relay verses Windows PC). PacifiCorp's recommended approach leverages both NERC's functional model and NIST together to benefit the cyber security of the BES. The core competencies of the NERC functional model are leveraged in selection of the Critical Assets. NIST's security controls core competencies are then leveraged in protection of the Critical Cyber Assets essential to the Critical Assets.
USBR	Page 9 line 10. Fundamentally, most entities have developed methodologies for the BES critical asset lists and critical cyber systems. They are in the process or have implemented significant modifications to their cyber asset and security protocols and hardware to protect those critical cyber systems. Accepting this approach will create the high probability that the entity which has achieved a level of compliance with the existing standards will not be compliant when the approach proposed by the drafting team is used to modify the existing standards. The registered entity must not reinvent its protocols and hardware for what may not be an improvement in the true vulnerability of the BES to failure of a critical cyber asset. The BES Functions

	described in the table are not specific enough to ascertain if a reliability impact for BES elements exists. Specific comments for the elements are described in question 2. In order to make it clear, the has to be specific determination that the subsystem will in fact have an impact on the BES Function. The language such as "whose compromise may result in" is not clear. The language should reflect a definite measurable impact "whose loss is demonstrated through system studies to result in" is specific and actionable.
PGE	Unclear. Shifting from an asset-based approach to a function-based approach would introduce additional ambiguity if each entity is made responsible for determining which functions are essential to maintaining an Adequate Level of Reliability. The determination of what constitutes an interconnection-wide Adequate Level of Reliability should include the input of the Regional Entities rather than being left to each individual entity. The approach in the concept paper would exponentially increase the scope of Cyber Assets potentially affected by the standard without providing entities with sufficient guidance to identify which assets are actually critical to the reliability of the BES. Such an approach would require the entity to undertake an extremely complex process which would be difficult to present to an auditor in an enforcement context. Additionally, the relationship between the reliability functions and the BES functions for which entities are registered is not clear.
FPL	1. We agree that the categorization by function is a good approach, however, as it is written there is still not a clear delineation of function vs. asset. The methodology as it is written, will still cause entities to go through a complete inventory of its cyber systems that touch the BES.
SWTDUG	I am writing on behalf of the Southwest Transmission Dependent Utility Group , a group of small utilities in the Southwest which occasionally intervenes in FERC proceedings to remind FERC that small utilities generally exempt from the Energy Policy Act of 2005 still exist. The purpose of this letter is to remind NERC and the Standards Drafting Team of the same reality. We will not comment substantively on the proposal for identifying various subsystems and this apparently new approach to identifying systems instead of cyber components and identifying them vertically down the system toward the ultimate consumer. Instead, we wish to offer a new construct we hope will be included in the effort. Just like improved technology to measure chemical components in drinking water does not, in and of itself, mean that that component in that quantity should be regulated, neither should the drafting team's ability to identify computer systems down the chain of communication into distribution systems change the regulatory structure with which we are currently living. In short, this exercise should not be an excuse for an attempt to expand jurisdiction and force entities that are not now registered

Question 1

	to become registered under the guise of "has a computer, will regulate". While we may have missed something in our review of the proposal, it seems to us that a seminal element is missing from your proposed inquiry. Simply stated, the study should identify the appropriate place in the arena of Registered Entities where proper control mechanisms and processes would best be placed to ensure that smaller adjuncts to the Bulk Electric System are not in a position to cause the problems that motivate this inquiry. Thus, the Regional Entity in question should not define the cyber system as an excuse to expand its jurisdiction but should look at the array of Registered Entities within that system as a template for installing protective facilities and measures. We hope that the Standards Drafting Team will accept this challenge and make it part of their inquiry and development of categorizing factors. Thank you for the opportunity to provide these informal comments on this proposal.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions. It is important that the subsystem criteria and subsystem examples be thoroughly vetted with the industry.

Question 2

2. In Table 1, the BES Reliability Functions listed in the "BES Function" column were not meant to be comprehensive. Are there any other functions we need to address and why?

Name	Comment
TNSK	As a Generator Owner and a Generator Operator the following information may not be readily available to support an adequate level of ALR; Contingency Reserve, Impacts on Frequency, Acceptable System Voltages, Nuclear Interface Requirements, System Operating Limits, Constraint Loading Requirements, and use of data supplied as it might relate to operational decisions. The Regional Entity will need to work with other entities to assess these functions.
XCEL	No
DOM	The BES functions are comprehensive, but to some degree they seem to be placing 'the cart before the horse.' The purpose of the CIP standards should be to establish requirements for the protection of cyber assets that support the BES, not for the protection of the specific BES functions themselves. In Table 1 for example, it is helpful to show BES systems and subsystems as shown in the first three columns just for reference, but it would be more helpful to breakdown the cyber system examples shown in column four in the same manner. In other words, show Cyber Functions, Cyber Subsystem Criteria, Cyber Subsystems Examples, etc., to give the reader a better feel for what the concept paper is aimed toward.
FMPA	For the reasons described in response to Question 1, FMPA believes that creation of a BES Reliability Function list that departs from the Functional Model, may add needless complication. We believe developing categories of "threats" is more appropriate. Such categories of threats could then be limited to functions in the functional model for assessment. For example, a threat of loss of "situational awareness" may be appropriate for some RCs/TOPs/BAs whose inaction or mistaken action due to lack of information or misinformation might cause "instability, uncontrolled separation, and cascading outages", but is not relevant from a security viewpoint to others, such as a DP, LSE or GO.
SWPA	No, in fact some of the examples are going beyond the scope of BES Reliability. For example, the Load Management Function is centered on distribution equipment that is not a part of the BES such as systems that control water heaters. If there is evidence that these systems control enough load to be material to BES Reliability, then NERC should establish a threshold level for aggregated water heater loads that is worthy of consideration. Also, the "Other" category either needs to be defined

Question 2

	or eliminated. This will lead to a wide open argument in an audit.
GTC	GTC questions the inclusion of the Load Management function as defined. Systems in support of "Load Control, Water heater, ac, etc." are outside of the purview of BES reliability. GTC also suggests further clarification of the "Other" category.
DYONYX	See comment in Question # 1. The functions, for purpose of identifying Critical Assets including "systems" which may be defined as Critical Assets, should be comprehensive and focused only on those specific functions that cause a direct impact on the reliability of the BES (see Security Guideline for the Electricity Sector: Identifying Critical Assets).
BPA	This list seems too large as is. BPA would be more inclined to reduce the list than add to it. A major point we found out with the Priority Pathways is keeping it simple is much better than complicating it. Lack of clarity for why criteria was included in the BES Subsystem Criteria. Lack of clarity of the relationship between the BES Function, BES Subsystem Criteria, BES Subsystem Examples, and Cyber System Examples. Does a system listed in one of the "Example" columns imply entities are required to consider this as part of our "target of protection"? How does this table of information relate to the paper production processes under NERC CIP? Page 12, BES Function: Control and Operation, lists "Inter-utility data exchange" as a BES Subsystem Criteria. We wonder if this "function" is related to EIDE, if so, how and why? Page 12, BES Function: Control and Operation, lists "Control centre functionality" as a BES Subsystem Criteria. What does this imply/mean?
SDGE	Table 1 seems to have a good selection of examples for BES Functions. I can't think of any other examples at this time.
GSOC	The table presented in section C, Table 1 is a good start in presenting the BES functions that affect the operability and reliability of the BES. In the table under BES Function 'Other', one function that should be considered is the fuel handling systems that supply the generating facilities, gas supply for larger Gas fired facilities, Coal Handling facilities, Hydro facilities head gates, etc. If these facilities were compromised it could result in a common mode failure for the whole facility. Cutting off the fuel supply for gas fired plants and hydro plants will have the same effect as tripping the breaker.

Question 2

BGE	Comment provided in the response to Question 1.
CUSMO	No, in fact some of the examples are going beyond the scope of BES Reliability. For example, the Load Management Function is centered on distribution equipment that is not a part of the BES such as systems that control water heaters. If there is evidence that these systems control enough load to be material to BES Reliability, then NERC should establish a threshold level for aggregated water heater loads that is worthy of consideration. Also, the "Other" category either needs to be defined or eliminated. This will lead to a wide open argument in an audit.
MH	Generation (which is not part of restoration, load balancing or contingency reserve) should be included in a reliability function with appropriate criteria for inclusion in the analysis. Where do Special Protection Systems fit into the reliability functions? They could be added as a reliability function which would be in keeping with CIP-002-1 or they should at least be added as a BES Subsystem Example under "Other" reliability function.
NST	We do not have specific functions to be added to the list that appears in Table 1. However, we recommend that this list be periodically reviewed and updated as necessary to reflect industry experience, evolving technology (e.g., Smart Grid), and possible future refinements to the current definitions of "reliability" and "operability" as they apply to the BES.
NPCC	At this time, we cannot think of any other functions.
RFC	No, an adequate sample has been presented.
IRC	No. However, the concept paper appears focused on Generation/Transmission Asset Owners and Operators and does not specifically address many BES functions typically found at ISO/RTO Control Centers which support Reliability Coordinator, Balancing Authority, and Transmission Operator (RC/BA/TOP) functions. Suggest further refinement and analysis of BES functions to specifically include and separately structure those functions provided by RC/BA/TOPs with wide-area or regional responsibilities as separate from those BES functions for Generation and Transmission System Owner/Operators per the NERC functional model.
AEP	The BES Function in Table 1 broadens the scope downward to include lower voltage transmission and distribution into the requirements of NERC-mandated cyber controls. This would exponentially increase the assets in scope without any significant

	benefit to enhance the security and reliability of the BES, as interruptions at this level would be local in nature without any wide area impact to the BES. For example, according to Table 1, Load Management Systems can be included into the loose definition of impacting the reliability of the BES. This is analogous to generation located on the distribution system that is not in scope of the BES. The graduated levels of cyber controls could apply to many more devices in stations, such as RTUs and PMUs; will this reduce our security exposure? Similarly, all generation necessary to serve load appears to be included into the ALR definition and this is a significant departure from the current standards. Could the drafting team provide clarification on this?
MGE	The list of "BES Functions" needs to be based on an established set of functions that are presently used within NERC and the utility industry. Registered Entities have applied countless hours of labor and spent huge sums of capital in being compliant with the current CIP-002-1 standard. Introducing new, unheard of functions will only lead to more confusion and slow down the implementation schedule. The Functional Model was designed to assist in designing NERC Standards perhaps that would be a useful reference. Each defined BES Subsystem (within the BES Function) needs to have a minimum level that is required to be met before applying this new methodology to it. An example would be Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more (as written in the current CIP-002-1 Standard). This will give a clear understanding of what threshold needs to be passed before applying this new methodology contained within the Concept paper. FERC Order 706, section 234 states that CIP-002 is the cornerstone of the CIP Reliability Standards because it acts as a "filter", determining whether a responsible entity must comply with the remaining CIP requirements. Suggest that the SDT have defined limits (filters) for all BES Subsystems, this will help all entities in ensuring that compliance with CIP-002 and be able to complete any following required CIP Standards.
WE	Wisconsin Electric does not feel there should be any additional functions to address. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	This is difficult to answer because it is not clear what the criteria for the BES Functions are, and the Functions are not clearly articulated. However, it appears that there are functions that are not truly critical to the reliability of the BES in Table 1, such as Contingency Reserve/Peakers (it is very unclear what this is referring to, as Contingency Reserves and Peakers are different things) and Load Management (seems only the part related to Load Balancing should be included). The methodology should recognize the diversity of contingency reserves (multiple units, purchases). Additionally, Constrain Management should not be in the table unless it is restricted to IROL management. Frequency Control (which is different than Frequency Response) should be added. If this methodology is to be used, more effort needs to be expended in developing industry consensus on what BES Functions should be included, working through established NERC committees and their subcommittees.

Question 2

SOCO	No and perhaps some of the functions can be combined.
E-ON	E ON U.S. suggests BES Reliability Functions are only those functions which 1) operate to prevent instability, uncontrolled separation, or cascading failures of the BES and 2) enable restoration of BES operation – rather than the comprehensive list provided in Table 1.
ATC	ATC believes that this table needs to focus on essential functions critical to preventing cascading outages / large blackouts and should not include protecting for an "Adequate Level of Reliability".
OMPA	Will a comprehensive list of BES functions be provided in the final concept paper based on the comments received?
TAPS	For the reasons described in response to Question 1, TAPS believes that creation of a BES Reliability Function list that departs from the Functional Model, may add needless complication. We also think that developing the list based on an ALR criterion is unduly broad. In contrast, defining the relevant BES Functions and Subsystems using a security focus (as opposed to an ALR focus), *i.e*., limiting them to BES Functions and Subsystems critical to avoiding instability, uncontrolled separation, and cascading outages, would allow for streamlining the applicability of the functions for the intended purpose, thereby appropriately narrowing the BES assets and cyber systems that warrant cyber protection. For example, the "situational awareness" function may be appropriate for RCs/TOPs/BAs, but is not relevant from a security viewpoint to others, such as a DP, LSE or GO. Again, unduly broadening the functions would inappropriately sweep into cyber security compliance unnecessary BES subsystems and cyber systems that support them.
GWA	It is not necessary for the list of functions to be exhaustive. The last row of Table 1 allows for other functions to be included. However, to prevent "Other" from becoming a catchall and potentially diluting security resources for functions with significant reliability impacts, it would be helpful to develop a description for "Other" that defines criteria for determining when a function should be included in consideration. The sentence, "Other Specific use systems whose loss or compromise may impact the reliable BES operation…" should be modified to "Other Specific use systems whose loss or compromise ~~may~~ <u>would reasonably be expected to</u> impact the reliable BES operation…"
MISO	If the list was not meant to be comprehensive, why are you asking if additional functions need to be included? Is the plan to have an exhaustive list at some point? We would discourage the drafting team from developing a standard that is so prescriptive that it would attempt to cover every conceivable situation. The drafting team should remember that this is not a specification but a reliability standard that should describe the "what" and not the "how" of protecting appropriate cyber

Question 2

	systems.
SCEG	Not to our knowledge. However it should be noted that if any functions are added these functions should only be those which support an adequate level of reliability (6 characteristics of the BES with an ALR)
RFC-CIP	Due to technological changes that will occur over time (e.g. smart grid technology), will entities have the flexibility to include additional functions that may be introduced after this version of CIP Standards becomes effective?
GEEI	No, but see the table below for clarifications needed.
LES	Yes, Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	This concept paper is confusing as well as this question. The concept paper indicates Table 1 only gives illustrative examples (see Section C) then in Section D this same table is suppose to indentify all BES Subsystems. Then this question here is looking for more illustrative examples. Perhaps the methodology should be reviewed to determine what is an essential BES function. MRO NSRS believes that Table 1 needs to focus on essential functions critical to preventing cascading outages / large blackouts and should not include protecting for an "Adequate Level of Reliability". However, the proposed approach does not provide more clarity than providing more specific criteria for asset selection under the current approach in the standards. More specific details would be required under any approach. MRO NSRS believes spending time adding clarity and specificity to the current standard is more productive.
MEC	No. MidAmerican is not aware of any additional functions that need to be addressed. MidAmerican is concerned with the complexity and overlap in the functions proposed. Providing more specific criteria for asset selection under the current approach in the standards would provide more clarity than the proposed approach. More specific details would be required under any approach. Spending time adding clarity and specificity to the current standard is more productive. The concept paper requires 14 pages to present just the concept of functions and still leaves many questions. The functions are not defined and would have to be synchronized with existing enforceable industry requirements that are already defined for BES operations. Without definition, functional categorization has the potential to expand the scope of Cyber Assets to be protected so significantly that the value of the cyber security investment is not maximized in mitigating risk.

Question 2

SCE	N/A – see comment to question 1.
APPA	See discussion of the Functional Model above under Q1. The SDT should consider whether BES Functions and BES Subsystems can instead be derived from the purpose sections and associated Requirements of NERC's other Reliability Standards.
PAC	No. PacifiCorp is not aware of any additional functions that need to be addressed. PacifiCorp recommends that the drafting team focus on providing clarity and specificity to the current standard by adding additional BES functions to the current evaluation criteria without abandoning an approach that has now been accepted and implemented by the industry.
USBR	Pages 10 through 14. The inclusion of Protective Relays used throughout the table as Cyber System Examples must be clarified to only include those relays that are addressable or programmable and would result in an impact to the BES. The inclusion of Plant Control Room(s) needs to be clarified as well. The inclusion of the under frequency scenario needs to be clarified as a system under frequency condition under a specific contingency condition as determined by studies. A Control Room is not a Cyber subsystem but may contain cyber equipment that may have an impact on the BES. The BES Subsystem criteria for "unacceptable system voltages" needs to be clarified as how that is determined and what the parameters are. The "Not meeting Nuclear Plant Interface Requirements" needs a caveat "if applicable". Constraint Management BES Subsystems examples Generation Unit(s) and Synchronous Condensers are not elements that meet the Glossary of Terms Definition for Constrained Facilities. These should be removed. The BES Subsystem Criteria for Control and Operation includes all Primary and Backup Control Centers used by Generator Operators "that have been registered in the NERC Registry. Since Registry is by function and not asset this automatically includes all control centers irrespective the size of the generation stations controlled. The selection of control centers would be by the role the control center plays in managing the BES. The BES Subsystem Criteria for Restoration includes all Generating units involved in restoration. Currently the selection of restoration units in many plans is not supported by study or test. The limitation should be those generating units essential to restoration as determined by system studies. The reference to Load (distribution feeders) needs to be clarified. The BES Subsystem Criteria for system stability indicates that Generation Resources need to be identified if they may compromise a number of events listed. This needs to be clarified how that would be determined to remove the best guess condition or needless conservatism.
FPL	We believe that most of the functions have been addressed and we agree that the list does not have to be fully comprehensive. We believe each entity needs to have some degree of discretion on what they think should be included in that list based on its specific system requirements. Although the list does not have to be comprehensive since any other system

Question 2

	that impacts reliability will be reviewed in other standards and thus included as needed.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions. It is important that the subsystem criteria and subsystem examples be thoroughly vetted within the industry.

Question 3

3. Does the methodology presented in Section D, Identification of BES Subsystems and Section F, Identification of BES Cyber Systems capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

Name	Comment
CLPUD	Yes, but see comment 1 above.
TNSK	All of the systems appear to be adequately captured. The reliability impact will have to be determined by the Regional Coordinator.
XCEL	Seems correct.
DOM	Again as mentioned above, the identification discussed in Section D is useful, but overemphasizes BES functions versus the cyber functions which should be the target of this approach. Also, applying the functions in Table 1 referenced by Section D with Section F seems to require that every device on our system will be evaluated at least once, and that that many devices will be assessed multiple times.
FMPA	See FMPA's responses to Questions 1 and 2, which describe why FMPA believes that the FPA Section 215 definition of reliability is more appropriate than ALR, and that categorizing threats is more appropriate than categorizing BES Reliability Functions or BES Subsystems.
SWPA	Yes, in fact it is too comprehensive and goes beyond the scope of the BES into distribution level equipment such as water heaters listed in the Load Management Function.
GTC	GTC believes that by tying the identification to reliability functions, all systems appropriate for protection are identified.
DYONYX	See comment in Question #1.

Question 3

BPA	This team felt that subsystems and cyber systems need to ultimately be defined by each utility on an individual basis. It is helpful that NERC lists specific examples for each subsystem. However, each utility may have exceptions or additions to the NERC list of subsystems and cyber systems. This may actually increase TFEs not decrease them.
SDGE	I don't see that a methodology is really presented in Section D for Identifying BES Subsystems. There is mention of application of "pre-defined criteria" for mapping, but I've read the paragraphs several times and can't really identify a clear methodology. Section F, however, does a better job of listing a fairly clear methodology to identify BES Cyber Systems. It's hard to say if Section F captures ALL of the systems that will need to be protected, but the examples listed represent a good start.
GSOC	See some of the examples listed in the answer to question 2 above for additional BES Subsystems to be considered. As far as the BES Cyber Systems, the focus has been and should be the specific BES Cyber System such as RTU, Electronic Relays, etc, Cyber systems associated with the communication needs to be considered. If the communication to or from Cyber Systems were compromised then it will definitely affect the operability of the BES. It would affect 'Situational Awareness', 'Control Center Operation', etc. Communications is out of scope in the NERC CIP Standards but these facilities should be factored in some capacity. These are the telecomm cyber systems that are located at the control centers, generating plants and substations that interface to the ESP.
BGE	Line 25: "centralized, automated, programmable area load shedding system": We can achieve this function using Advanced Meter Disconnect function and also using Demand Response devices such as Smart Thermostats controlling Air Conditioners. 1. Does this mean both AMI and Demand Response systems are automatically considered as a Critical Cyber System? 2. Any provision/controls such as maximum load that can be shed, and the time period in which the load is shed gradually instead of instantaneously, make these systems non-CIP or at least low Cyber Impact systems? 3. For AMI / Demand Response Systems it will be very helpful if the identification criteria is explained with a specific example with load, time parameters etc. If amount of load does not matter, please state this explicitly. 4. If safeguards have been put in place to keep a subsystem within Adequate Level of Reliability, does that system then fall under the CIP guidelines?
CUSMO	Yes, in fact it is too comprehensive and goes beyond the scope of the BES into distribution level equipment such as water heaters listed in the Load Management Function.

Question 3

MH	Under "Control and Operation" AGC should also be listed as a BES Subsystem Example in addition to Cyber System Example. Cyber system components could be AGC (as part of EMS or separate), station controllers and unit controls. Where do Special Protection Systems fit into the reliability functions? They could be added as a reliability function which would be in keeping with CIP-002-1 or they should at least be added as a BES Subsystem Example under "Other" reliability function. Under "Other" reliability function the following two BES Subsystem Examples should be removed as they are targets of protection (support subsystems) and not BES Subsystems: "Support systems used to modify cyber systems "and "Physical Security System". All components in a BES Subsystem should not automatically inherit the categorization of the overall BES subsystem. If many units are part of the BES subsystem, then the assessed impact could be Minimal (very low) for an individual unit. Redundancy (often mandatory requirements in other reliability standards) should be considered by individual Responsible Entities as part of their consideration as it may reduce the impact of an individual BES asset. Master ends of BES subsystems may be categorized higher than individual remote end BES Subsystems. Responsible Entities should be allowed flexibility to properly determine the range of impacts and the resulting categorization of the BES assets. Provision for this flexibility should be provided in the overall procedure for BES subsystem categorization. Any impacts for any common mode failure of cyber subsystems should be addressed in the categorization of cyber systems. Consideration should be given for a categorization level where no mandated security controls are required (Level for None).
NST	Regarding the identification of BES Subsystems, we recommend that the SDT clarify whether or not it anticipates that all BES Subsystems would be considered and characterized (High, Medium, Low) using the proposed methodology. If not, we recommend the SDT discuss what types of systems would typically be excluded (i.e., what type of BES elements or facilities perform or support functions that do not support the characteristics of ALR). Regarding the identification of BES Cyber Systems, we recommend that the SDT consider carrying forward CIP-002-1's concept of identifying cyber systems that are essential to the operation of one or more BES Subsystems or to the performance of BES reliability or operability functions. We believe this qualifier is presently and would in the future be useful to help distinguish BES Cyber Systems that directly perform or support BES functions from cyber systems that play a supporting but not a direct role (referred to as "Interconnected Cyber Systems" in Section I, "Defining The Target of Protection"). Cyber systems that could, if compromised, be used to directly disable or impair BES Subsystems and/or BES functions should also be identified as "BES Cyber Systems" even if those cyber systems are not deemed "essential."
NPCC	Yes, the methodology in Sections D and F capture all of the systems that will need to be protected to achieve an acceptable level of reliability. No other issues need be considered.

Question 3

RFC	Yes
IRC	Generally Yes. The concepts proposed within this section create valid selection criteria for the identification of BES Subsystems that have the capability for impact to the reliability of the BES from a regional or multi-regional approach. Reliability Coordinators, Balancing Authorities and/or Transmission Operators (RC/BA/TOPs) currently do not have the necessary Authority or "Safe Harbor" to determine what Registered Entity assets within their areas may be a risk to reliability of the BES. Although these Registered Entities are interconnected via interweaving cyber communications and data processing systems, the RC/BA/TOPs currently have little say in what the Registered Entities declare as CCAs. Additionally the RC/BA/TOPs do NOT have sufficient staff with the required skills and knowledge to perform the needed security risk assessments necessary to make these key determinations. While absolutely essential for success of the risk assessment process, the current skill sets of Electrical Power System Engineers currently found in most operations and planning groups do not include sufficient abilities to perform the cyber system and network security risk assessments needed to successfully support this type of regional oversight program. The costs associated with establishing this initial capability and sustaining the ongoing studies and assessments annually required to meet compliance may be significant as the security analysts, architects and risk managers with backgrounds in Electrical Power Systems are a scarce resource nationwide. It has been said that the North American Grid is the most complicated machine ever built but the regions are the second-most complicated machines. Any standard requiring the RC/BA/TOPs to perform the analysis proposed in these sections, must also address funding to pay for that support which may be far above their current operational budgets today.
AEP	The paper talks of Adequate Level of Reliability (ALR) but then continues to include issues just impacting reliability. Every outage, or every system that is unavailable 'impacts' reliability, but the loss of that system does not necessarily reduce reliability to below 'adequate' levels. Situational Awareness is another term used, but not really defined. All data, even the current temperature and the temperature forecast, provides "Situational Awareness," but loss of a thermometer does not degrade the transmission system to a level below the ALR. The utilization of an open model, such as described in this concept paper, may produce unintended or onerous results.
MGE	In Section D, it appears that BES Subsystem(s) are captured and that is what the industry appreciates, a clear cut, defined area that will help entities comply with the Standard. Perhaps the SDT should allow the Applicable Entities to use this as a minimum level and afford entities the ability to establish other BES Subsystems that are equally effective and efficient and unique to their system.

Question 3

	Section F, Due to the wide assortment of technology that is used within the Eastern, Western interconnections, and ERCOT the SDT should allow the Applicable Entities to use this as an example or allow them to establish other BES Subsystems that are equally effective and efficient.
WE	Wisconsin Electric's opinion is that all BES cyber systems have been captured in Section D. We do encourage the continued use of probability of occurrence of a cyber attack to limit protection of systems that have little or no impact to the BES. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	The methodology will not only capture all of the systems that need to be protected, it will capture too much. The methodology is not selective enough. Additional guidance may be necessary to limit the scope of BES cyber systems. For example, it may need to be stated that only real time monitoring and alerting systems are in the scope since those can affect Grid operability. Also, following the logic in sections D and F, the steps for determining cyber systems in scope appear to be: 1) identify BES Essential Functions; 2) derive BES Subsystems (including BES **cyber** subsystems) using the list from step 1; 3) derive BES cyber systems from the step 2 list; 4) derive a list of Cyber systems supporting BES cyber systems. The proposed BES Cyber systems and supporting BES Cyber systems identification process significantly expands the number of cyber systems that may be affected by this guideline and hence by the NERC CIP requirements. Consideration should be given to using the TPL standards to identify what equipment is essential to supporting the BES Functions specified in this methodology and whose supporting systems should be considered BES Subsystems.
SOCO	Yes. It appears to cover them all. We understand the drafting team will next consider the degree to which these systems and subsystems will need to be protected.
E-ON	The methodology presented in Sections D and F is overly inclusive and appears to capture far more than those systems essential to insuring BES reliability
ATC	A cyber attack should not be tied to the NERC definition of an ALR. A cyber attack is a high impact low probability event and would be less probable than a NERC category D event. A category D event would not provide an ALR.
TAPS	See response to Questions 1 and 2.
GWA	Given the evolution of the industry it seems reasonable to assume that the list is not comprehensive, and that should be stated. One example of an omission is a Wide Area Measurement System (a BES Subsystem) that may evolve with the

Question 3

	deployment of more synchrophasors in the Bulk Electric System. The document should be as comprehensive as possible, with an understanding that not every BES System and Subsystem can be included. The systems listed should serve as examples to allow other types of Subsystems and Cyber Systems to be identified by Registered Entities.
MISO	The methodologies are not clear what is being protected against and appear to assume because a cyber system supports a BES asset that it will need to be protected automatically. The purpose of a reliability standard is protect the BES not the associated cyber systems. Protecting the cyber systems often supports the main purpose but is not always necessary to protect the asset. As an example, most generators require a manual operator intervention to re-synchronize to the grid and startup once they have tripped off-line. Does the need for manual intervention, thus, obviate the need for protecting some of the associated cyber systems? Thus, these methodologies will likely identify more BES Subsystems and BES Cyber Systems that need to be protected than necessary to maintain a reliable grid. The drafting team should solicit for industry experts with field operation experience to assess to what level the actual BES asset could be compromised.
SCEG	Yes
RFC-CIP	Same as comment for Q2. Will entities have the flexibility to add Subsystems and Cyber Systems not already included in the Standard's lists as technology changes?
GEEI	The issue to be considered is if you have a small generating station but is Interconnected power system how do you identify BES Cyber systems even for a small system
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	The methodologies presented in Sections D and F do not capture all of the systems that will need to be protected since the Adequate Level Reliability criteria was not applied correctly. In Section F, the MRO NSRS agrees the full target of protection should be identified especially before considering other cyber system components; it's unclear what these other cyber system components would be since Section F introduces them but does not explain what these systems are.
MEC	Section D does not provide a clear methodology and creates a new concept of subsystem without subsystems definition or clarity. Section D points out there may be cyber systems that may perform or support the BES on a wide-area basis that may or may not be associated with any specific BES asset. The concept paper proposes categorizing these as both a BES

Question 3

	Subsystem and a Cyber System creating confusion. A more direct, achievable methodology is to build on CIP-002 R3 where Cyber Assets essential to the operation of the Critical Assets are identified. Requirement 3's list of examples already include some cyber systems that are not associated with any specific BES asset alone but do support the BES on a broader scale. Refining these examples would achieve the objective of capturing the systems that need to be protected.
PSEG	Table One, Other section (Line 46-50) identifies "Support systems used to modify cyber systems" as BES subsystem and cyber system examples. This type of broad definition will again lead to the confusion and ambiguity currently associated with CIP-002, Version 1. The drafting team must be must more specific with descriptions such as these.
SCE	N/A – see comment to question 1.
AWEA	A more important question is "How will the BES reliability impact of a specific Subsystem be assessed?" Insufficient information of the assessment methodology is provided to judge any aspect of the process.
APPA	See discussion of the Functional Model above under Q1. The SDT should consider whether BES Functions can instead be derived from the purpose sections and associated Requirements of NERC's other Reliability Standards. Identification of BES Subsystems and Cyber systems could take place through the same process. The step that is new appears to be the reverse engineering to track the reliance of many diverse BES Systems on common use Cyber systems. It would appear that registered entities may need to perform this mapping of BES and Cyber systems in both directions, top-down and bottom-up.
PAC	Section D does not provide a clear methodology and creates a new concept of subsystem without definition or clarity of what subsystems are. Section D points out that there may be cyber systems that may perform or support the BES on a wide-area basis that may or may not be associated with any specific BES asset. The concept paper proposes categorizing these as both a BES Subsystem and a Cyber System. This creates confusion. A more direct, achievable methodology is to build on CIP-002 R3 where Cyber Assets that are essential to the operation of the Critical Assets are identified. Requirement 3's list of examples already include some cyber systems that are not associated with any specific BES asset alone but do support the BES on a broader scale. Refining these examples would achieve the objective of capturing the systems that need to be protected.
USBR	Page 15. No. The methodology would indentify elements that would not or may not have an impact on the BES. The list does not clarify that the impact the BES must be based on a factual assessment. Section F also now includes Alarm functions and

Question 3

	Feeder Rating systems.
PGE	This methodology could inadvertently capture more than what is required to maintain BES ALR. It is unclear how the Regional Entity or NERC will hold entities accountable for the scope of BES Subsystems or Cyber Systems identified.
FPL	As stated in responses 1 and 2, we believe this methodology should provide guidelines and does need to capture all of the systems since this will be done in other standards such as the TPLs. Table 1 and the flow chart in figure 2 are very helpful. Section D is confusing in that it mixes topics i.e. subject heading is identification of BES subsystems yet also talks about cyber systems.
TECO	We would encourage the SDT to map these functions back to the NERC defined BES Reliability Functions and include operating staff in the review of these. Table 1 does seem to address all the systems we are aware of. Q1 and Q2 deal with functions. Our staff is not comfortable with the definitions of the functions and would like them to map back to the NERC definitions.

Question 4

4. Section E, Impact Mapping of BES Subsystems proposes that all identified BES subsystems be mapped into categories based on pre-defined criteria that reflect their impact on the reliability and operability of the BES. This mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach, and if not, what alternative suggestion do you have?

Name	Comment
CLPUD	Yes.
TNSK	As a Generator Owner and a Generator Operator we do not have the information required to classify events based on the proposed graduated impact scale. We would like to work with the Regional Coordinator to perform this impact analysis to support the goal of ALR.
XCEL	Yes
DOM	The Operating Reliability Event Categories cited as an example are based more on loss of entire BES systems (e.g., lines, generators, networks) and not necessarily subsystems. It is difficult to predict how this concept could then be used to prioritize the cyber systems that support critical BES subsystem infrastructure. Furthermore, as the categories increase in severity, the criteria are based more on the simultaneous loss of several components or systems. The existing CIP standards were not adequately designed to address multiple contingencies. If addressing multiple contingencies is now desired, the paper should address contingency levels for cyber component directly, rather than tying these to a BES subsystem ranking. It would be difficult to apply the mapping described to components that could be operating in several completely different time frames. An RTU, which has been used in several examples as an example of a critical cyber system, can operate to supply real time data acquisition and control and, at the same time, supply accumulator data for other functions. Furthermore the criticality of a component such as this will also vary from day to day, if not hour to hour, as load and exact system configurations change. Simply put, a mapping of high on a component one day could be seen as low on another day. It is not clear how this concept will be useful in establishing criteria for cyber system reliability
FMPA	See FMPA's responses to Questions 1 and 2. FMPA believes categorizing threats is a more appropriate approach than defining new terms such as BES Reliability Functions and BES Subsystems. However, FMPA does agree that the threats ought to be measured against pre-defined criteria that measures the possibility of malicious control of a cyber system causing

Question 4

	"instability, uncontrolled separation, or cascading failure". For instance, the threat of loss of supply could be measured against the Contingency Reserves of the Reserve Sharing Group, or against the largest single loss of source in a region, as a measure of the threat of "instability, uncontrolled separation, or cascading failure".
SWPA	Yes, at a high level we agree with this approach. However, we need to know what the "pre-defined criteria" are. The NERC Guideline for the Electric Sector - Identifying Critical Assets has already given us "pre-defined" criteria to follow when identifying assets that are critical to BES reliability. Let's first prove that the current efforts are not effective or NERC should simply tell us what systems are critical and take the guess work out of it. The industry is spending a lot of valuable resources chasing this moving target. Without any details it appears that this approach will force all registered entities regardless of size or location to identify all of their BES systems and then be responsible for documenting a certain level of protection on all of these systems again. While we do agree that it is in our own best interest to secure all of our cyber systems, we do not agree that they all should be monitored for compliance to mandatory standards and financial penalties. This approach is not consistent with other reliability standards such as FAC-003 Transmission Vegetation Management Program and PRC-023 Transmission Relay Loadability. These standards only apply to facilities above 200 kV or those that are identified as critical to BES reliability. They don't require a minimum level of requirements on all facilities and these standards are assigned "High" VRFs, while most of the CIPs are all "Low" to "Medium" VRFs. If the CIP Standards are allowed to reach into low-voltage systems that control water heaters, how can we ignore vegetation management on distribution lines where local reliability issues are proven?
GTC	GTC agrees with this approach and believes that mapping using pre-defined criteria should significantly reduce the effort and controversy involved in categorizing BES subsystems over a "define-it-yourself" methodology. However, gaining consensus on the pre-defined criteria will be a considerable undertaking.
DYONYX	We are very concerned by the "to be defined" "pre-defined criteria" in assessing the level of impact.
BPA	For the most part we agree with this approach. Our suggestion is to add to the existing options of High, Medium and Low impact a 4th option – Non-applicable. There needs to be a way to identify systems that have zero impact on the BES and a Non-applicable option would meet that need. – Bulk power system event classification? – What is the local impact – High med low are subjective. What do these mean to us? – Regions should figure out what is high impact for their areas. Page 16, lines 10-20, what are they trying to say here?

Question 4

SDGE	It seems like a good approach, but will ultimately depend on the pre-defined criteria and the categorization levels that are identified.
GSOC	The approach is realistic but reaching agreement on pre-defined criteria may take some time and considerable discussion. The big concern is how some of the entities will be able to determine the mapping for their facilities. For example some of the IPPs and smaller Utilities do not have the capability to determine the impact of their facility on the BES, other than some of the obvious items, such as they are a blackstart facility included in the regional blackstart plan or the facility is greater than the BA Contingency Reserve allocation. They do not have the ability to conduct power flow and contingency analysis studies. The RC should be the responsible entity to determine the impact of the assets within their RC footprint and categorize them into high, medium and low. It is the RC who has overall responsibility for reliability. In some regions the RC conducts the studies and informs the registered entity which of their facilities is a Critical Asset. Under this new suggested BES mapping the RC should determine the asset mapping into high, medium or low.
CUSMO	Yes, at a high level we agree with this approach. However, we need to know what the "pre-defined criteria" are. The NERC Guideline for the Electric Sector - Identifying Critical Assets has already given us "pre-defined" criteria to follow when identifying assets that are critical to BES reliability. Let's first prove that the current efforts are not effective or NERC should simply tell us what systems are critical and take the guess work out of it. The industry is spending a lot of valuable resources chasing this moving target. Without any details it appears that this approach will force all registered entities regardless of size or location to identify all of their BES systems and then be responsible for documenting a certain level of protection on all of these systems again. While we do agree that it is in our own best interest to secure all of our cyber systems, we do not agree that they all should be monitored for compliance to mandatory standards and financial penalties. This approach is not consistent with other reliability standards such as FAC-003 Transmission Vegetation Management Program and PRC-023 Transmission Relay Loadability. These standards only apply to facilities above 200 kV or those that are identified as critical to BES reliability. They don't require a minimum level of requirements on all facilities and these standards are assigned "High" VRFs, while most of the CIPs are all "Low" to "Medium" VRFs. If the CIP Standards are allowed to reach into low-voltage systems that control water heaters, how can we ignore vegetation management on distribution lines where local reliability issues are proven?
MH	Alternative 1: If the impact mapping of BES Subsystems is based on very prescriptive criteria which provides minimal flexibility for the individual entity to categorize their BES assets then the revised CIP Standard should not include the procedure outlined in the concept paper; rather the revised CIP Standard should just document the criteria table for industry to use to assign the BES impact. The concept for categorizing cyber assets would be used by the team to develop the appropriate table(s). This simple approach would avoid industry investing effort in low value activities such as documentation.

Question 4

	Alternative 2: If the impact mapping of BES Subsystems provides sufficient flexibility for individual Responsible Entities to properly evaluate the impact of their BES assets, then they can determine the appropriate BES Subsystem categorization. Responsible Entities would need to document their processes, assumptions and considerations. Examples: Redundant assets might be categorized lower due to redundancy than if only a single asset exists, or for AGC, the master end might be evaluated higher than the plant controllers or individual unit controllers based on MW impact. Manitoba Hydro favours this approach provided that there is value in more appropriate application of security controls by having performed the additional analysis. For either alternative, consideration should be given for the followings issues: – All components in a BES Subsystem should not automatically inherit the categorization of the overall BES subsystem. If many units are part of the BES subsystem, then the assessed impact could be Minimal (very low) for an individual unit. Redundancy (often mandated by other reliability standards) should be considered by individual Responsible Entities as part of their consideration and it may reduce the impact of an individual BES asset. Master ends of BES subsystems may be categorized higher than individual remote ends of BES Subsystems. – Responsible Entities should be allowed flexibility to properly determine the range of impacts and the resulting categorization of the BES assets. Provision for this flexibility should be provided in the overall procedure for BES subsystem categorization. – Any impacts for any common mode failure of cyber subsystems should be addressed in the categorization of cyber systems. Consideration should be given for a BES subsystem categorization level where no mandated security controls are required (Level for None).
NST	We are concerned that both defining and applying a comprehensive set of pre-defined criteria intended to facilitate a lookup-based categorization of BES Subsystems could prove a daunting and time-consuming task. Further, we believe it may not be either appropriate or desirable to essentially remove local entities' engineering expertise and judgment from the process of evaluating a given BES Subsystem's impact on BES reliability or operability. However, at the same time we support the goal of defining and applying an industry-wide set of metrics for BES Subsystem categorization, as it should result in a more consistent set of results with fewer regional and entity-specific differences in how BES assets are assessed for criticality than seems to be the case under the current version of CIP-002. Our recommendation is to conduct several trials of the proposed function and criteria-based categorization of BES Subsystems once an initial draft set of criteria has been completed. Trials should be conducted among different size companies, in multiple regions, with non-binding results, to gain a sense of whether the proposed methodology yields the type of results anticipated by the SDT.

Question 4

NPCC	Agree with this approach.
RFC	We agree.
IRC	Agree with approach. Comments for Section D above are also applicable here.
AEP	Performing pre-mapping and applying generic predetermined "risk assessment" can be inefficient and may result in undesired outcomes. This could contribute to either over or under securing individual systems. We would be better served by enhancing the current base of cyber security standards in order to increase clarity.
MGE	No. The "pre-defined criteria" has not been defined by the SDT and this question cannot be answered. The BES Subsystem is a subset of all programmable electronic devices (to include communication networks) that has had a process applied to it (methodology) and has been determined to require additional electronic protection against a possible malicious attack that could disrupt that programmable device that effects the BES.
WE	Wisconsin Electric does not agree with this approach based on the removal of a risk based analysis of the asset/system using probability of occurrence. We also feel this approach would add more interpretation issues as well as audit complexity. We would prefer to utilize current methodology as defined in CIP 002-1 with further refinement of the risk based methodology. If the proposed approach is used, there should be a reduced set of standard requirements for CIP that need to be complied with. As an example, Wisconsin Electric would not agree with an approach to require full compliance to all CIP standard requirements but have a lower violation severity level for non compliance due to the lower impact on reliability of the subsystem. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	As long as the scope is clear, the differentiation between the controls on the different levels are significant, the criteria are clear and correct and the number of levels are appropriate, the concept itself is sound. However, it is difficult with the information provided to assess whether this can be implemented correctly.
SOCO	No. As noted by FERC in Order 706 (Paragraph 111), "flexibility and discretion are essential in implementing the CIP Reliability Standards" and "implementing those Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand." FERC further noted in the same paragraph that "[c]yber security problems do not lend themselves to one-size-fits-all solutions." Based on these same principles set forth by FERC, NERC should consider not adopting pre-defined static criteria for mapping the impact of BES subsystems. Rather, NERC should

Question 4

	provide criteria that would be applied unless the responsible entity documents through a sound engineering study that such BES subsystem should be placed within another category.
E-ON	E.ON U.S. does not agree. E. ON U.S. suggests BES subsystems be defined as systems the failure of which would lead to instability, uncontrolled separation, or cascading failures of the BES or impede restoration of BES operation
ATC	ATC does not agree with this approach because the team has removed the ability to determine the probability and severity of an event's occurrence. We agree that entities need to understand the impact of an event but that the likelihood of that event needs to be included in the equation. The failure to include the probability of the event will result in a drastic increase in cost with no meaningful benefits to the reliability of the BES. ATC also believes that the paper needs to provide more information as to why this approach is being proposed and the improvements over the existing process. We believe that these changes were not directed by FERC nor are they needed to address other aspects of Order 706.
TAPS	See response to Questions 1 and 2.
GWA	GWA members support an approach that considers reliability impacts of BES subsystems, pending review of the actual criteria once they have been defined. (see p. 16)
MISO	A BES subsystem either supports reliability or it does not. It seems that the current Critical Asset and non-Critical Asset approach would still be fitting.
SCEG	Yes
RFC-CIP	It seems to be consistent with the approach used for determining the degree of impact applied to Cyber Systems. Section E suggests categorizing event impact as High, Medium, and Low. It also suggests using criteria similar to NERC's Bulk Power Event Classification Scale which for Operating Reliability Events uses five categories. The drafting team should consider mapping the five categories to High, Medium, and Low. Implementing five impact categories would be unmanageable and not provide an improved security model.

Question 4

GEEI	Yes, in theory. In practice, a similar function does not imply the same level of impact. Whether due to other mitigating automatic or manual controls, the loss of a function in one BES subsystem at one facility may not have the same level of impact on reliability as the loss of the same function in a similar BES subsystem at another facility.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No. It is unclear what value would be added by having multiple classifications. FERC Order 672 says that standards should be clear and unambiguous.
MEC	No. MidAmerican is concerned with the complexity in mapping to the categories proposed. The proposed concept does not provide more clarity than providing more specific criteria for Critical Asset selection under the current approach in the standards. More specific details would be required under any approach. It will be more productive to add clarity and specificity to the current standard.
MMPA	The approach is good as long as the "pre-defined criteria" is appropriately gauged. If the criteria is set too low it will encompasses assets that do not impact the BES. If it is set too high, than it may miss assets that could impact the BES.
SCE	N/A – see comment to question 1.
AWEA	The "pre-defined criteria that reflect their impact on the reliability and operability of the BES" are critical. Without knowing what the criteria will be, it is of limited use to judge the process. One concern is that the comprehensive/bottom-up process outlined in the paper may devote too much attention to smaller-scale components of the power system that, due in part to their small size, would be extremely unlikely to affect the reliability of the bulk power system. Some type of initial screening process that excludes generators and other grid components that fall below a certain size/importance threshold and thus are unlikely to affect grid reliability would be a useful step to ensure that the scarce resources available for securing the grid are devoted to steps that will yield the most benefits. Variable generators may also merit exclusion since they are typically treated as providing little or no capacity value to the power system. Taken literally, the guidance in this document would require that virtually all generating units, even small, variable resources like wind and run-of-river hydro, etc., be designated as "critical assets." Since these units, no matter how small or non-dispatchable, can be started in 15 minutes or less and can result in some amount of underfrequency if they are taken out of service unexpectedly, they would fall under the criteria specified under the reliability functions "Contingency Reserve/Peakers" and "Load Balancing, Frequency Response/Support." But these criteria are not consistent with power industry practice or

Question 4

	needs. During a generation shortfall, what is needed is firm dispatchable capacity. An intermittent resource, like wind, that provides only energy and is incapable of being dispatched or committed at any specific output level, should not be considered a critical resource. With respect to generation, we think the characterization of "critical asset" should be based principally on committable and dispatchable capacity that can be exercised by the generation asset. A reasonable lower limit (e.g. a certain and relatively high number of MW of committable dispatchable capacity) should be used to make that designation. Wind assets obviously should be put in a different category than a dispatchable combined cycle or coal unit of similar maximum output.
APPA	See response to Q3.
PAC	No. PacifiCorp is concerned that the process of applying the pre-defined criteria to the BES subsystems will only add additional confusion to the industry and may introduce opportunity for a number of different interpretations by responsible entities. PacifiCorp also feels that finding agreement between the industry and the drafting team on acceptable criteria will be difficult and may delay needed revisions to the current standards. PacifiCorp feels it would be more productive to add clarity and specificity to the current standards. It should be noted that a similar impact mapping process could be used within the current methodology by first identifying the BES critical facilities, identifying the critical cyber systems supporting that facility, and then accessing the impact of that system based upon the impact to that facility and the probability of an occurrence of a security event.
USBR	No, the mapping is already needed as part of the existing version of the CIP standards. An alternative is not needed.
PGE	It is difficult to comment on the impact of this approach without knowing anything about the "pre-defined criteria." The specificity and clarity of those criteria will be critical to this approach.
FPL	Although we agree with the general approach, we believe additional language should be provided regarding risk assessments and definitions of threat basis. It is important that any pre-defined criteria are not overly restrictive since it will depend on the different systems of each company and varying situations across the regions.
TECO	We are concerned that the criteria for the definitions must be clear, simple, and not subject to interpretation.

Question 5

5. Section E, Impact Mapping of BES Subsystems provides an example of three impact levels: High, Medium, and Low. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems, and why?

Name	Comment
CLPUD	No opinion.
TNSK	I would recommend 2 levels, especially if these translate to different hardening requirements to keep the implementation less confusing and manageable. Potential constraints or remedies for unregulated Generator Owner and Generator Operator non-utility entities should be considered.
Xcel	Additional level of "None" should be added as a fourth.
DOM	Based on having to evaluate every piece of equipment, 2 levels perhaps (high or low), is more appropriate.
FMPA	See FMPA's responses to Questions 1, 2 and 4. As FMPA explains in those responses, FMPA believes that "threats" ought to be mapped instead of BES Subsystems. FMPA also believes that only two levels are needed: 1) critical, and 2) non-critical, as was the original intent of the standard. FMPA believes that the FPA Section 215 definition of reliability ought to be used as the "yard-stick" to determine if a system is critical or non-critical. FMPA believes that a critical cyber system should be regulated by the standards and the measure for whether a system is critical or not is to determine through threat analysis if a cyber system can be maliciously used to cause "instability, uncontrolled separation, or cascading failure". All other cyber assets would be non-critical and not regulated by the standards.
SWPA	There needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current approach will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
GTC	GTC believes that 3 levels are appropriate.

Question 5

DYONYX	We believe only two levels are needed as currently defined, Critical or Not-Critical.
BPA	4 Levels – High, Medium, Low and Non-applicable. See Comment #4
SDGE	I believe that 3-4 levels would be best for impact mapping. Any larger number of impact levels would probably be too confusing to implement.
GSOC	The main objective is to determine the impact the asset has on the reliability and operability of the BES, therefore, the three levels of impact is a good starting point. We do not see having any more levels, either the asset has an impact or it doesn't and having the three levels helps to establish the degree of the impact the asset has on the reliability and operability of the BES.
CUSMO	There needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current approach will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
MH	Manitoba Hydro suggests a minimum of three (3) and a maximum of five (5) impact levels. Impact levels: High, Medium, and Low may not be sufficient for BES Subsystem impact categorization; however, too many levels could be confusing and difficult to implement. All components of a BES Subsystem should not necessarily inherit the BES subsystem impact level. Individual components of the BES Subsystem may require a lower impact level; therefore, an additional impact level may be required (four (4) levels). Consideration should be given for a BES subsystem categorization level where no mandated security controls are required (Level 5 Negligible, Minimal or Very Low). If this additional level is not available for BES components, then all BES Subsystem components will inherit the higher impact which may lead to inappropriate application of security controls. All common mode impact introduced by interconnecting cyber assets should be addressed by the target of protection and cyber impact analysis.
NST	We believe three impact levels is an appropriate number, as it reflects a recognition there are differences among BES Subsystems in terms of their relative importance to reliability and/or operability, and that it is appropriate to then account for these relative differences when establishing a set of required security controls for associated Cyber Systems.

Question 5

	We also consider three to be an appropriate number of levels by virtue of the fact that FIPS Pub 199 the NIST risk management framework, both referenced by the concept paper, are based on the use of three-level information and information system categorizations. At the same time, we believe three is the maximum number of levels that should be defined, as using more levels would in our opinion add considerable complexity to the categorization process without a commensurate improvement in cyber security.
NPCC	We suggest a fourth level, which addresses the highest of the High. We suggest "Critical" for this fourth level.
RFC	We agree with three levels.
IRC	Support the current concept of High/Med/Low as depicted in the concept paper.
AEP	Without the benefit of seeing how the impact levels affect the controls, it is difficult to determine how the granularity would be applied. Application of cyber controls on graduated levels may result in increased uncertainty as to what controls apply; what will an auditor judge vs. our opinion? This is difficult enough currently with basically a binary decision system. However, a graduated approach is a good concept if the scope was focused on "essential" systems and not every system directly or indirectly associated with the BES operations. If a graduated approach is utilized, there should be a choice for "no impact."
MGE	The BES Subsystem is a subset of all programmable electronic devices (to include communication networks) that has had a process applied to it (methodology) and has been determined to require additional electronic protection against a possible malicious attack that could disrupt that programmable device that effects the BES. There should be two levels, critical and non critical. The SDT assumes that all BES Subsystems have an impact on the BES. As in the presently written CIP-002-1 methodology, a system is set up to see if an item is critical or not. This is not present in this concept paper. An example might be a 15MVA generator connected at the Distribution level, connected to SCADA/EMS and not blackstart capable. This concept paper would probably say it is in the "Low" impact category. Why? Because the Concept Paper (SDT) assumes it should be. There may be items that don't fall within this BES Subset and would be placed in the "non critical" category.
WE	Wisconsin Electric feels an additional level of "no impact to the BES" should be defined. Wisconsin Electric also supports comments submitted by EEI on this subject.

Question 5

DUKE	No. Another level is needed for subsystems that would have a negligible impact on the reliability or operability of the BES. While these subsystems would need to be reviewed and evaluated, and may theoretically have an impact on the BES, that impact and the probability may be so small that the resources should be applied elsewhere.
SOCO	A fourth level of none or not-applicable is needed for cyber items that are in the Target of Protection but have an insignificant impact on the operability of BES Cyber Systems or the reliability of the Bulk Electric System. As an alternative, because the definitions for medium and low levels are very similar, NERC should consider combining the medium and low levels and having the following three levels: High, Low, Not Applicable.
E-ON	One. Medium and low risks are irrelevant. Only cyber systems the loss of which could lead to instability, uncontrolled separation, or cascading failures of the BES, or impair the ability to restore BES operation, are relevant
ATC	ATC does not object to the categorization of "High", "Medium" and "Low" but that entities must be allowed to consider the probability of an event. In addition entities must be able to consider their security practices along with their current cyber and physical protection investments. If this approach is to be implemented then we believe that either a fourth category should be added that would represent "no" impact on the BES or that the group follows the five event categories currently used by NERC. (Event categories 1-5) ATC also believes that the SDT should identify the potential cyber and physical protection that will be assigned to each category ("High, "Medium" and "Low").
OMPA	OMPA agrees there should be the availability of levels or degrees of impact rather than a one-size fits all; however, OMPA believes that an option of "no impact" should be identified in the impact mapping process. Is this assumed that if the process, equipment or facility has no impact that it is simply not listed? Risk is typically determined by looking at both probability and impact. OMPA recommends the addition of "probability" in the process vs. looking only at the "impact" or severity of the event or occurrence. This assists an entity with prioritizing the processes, equipment, facilities, systems that resources will be assigned such that they are consistent with the overall risk to the BES.
TAPS	The Concept Paper's proposed mapping of BES subsystems for high, medium, and low impacts incorrectly assumes that the cyber systems supporting each such BES subsystem has an impact on reliable operation of the BES that merits some (albeit low n the case of low impact systems) level of regulation of cyber security protection. TAPS believes a fourth category of minimal impact, *not* meriting regulation by mandatory cyber protection standards, should be added. Alternatively, in light of the

Question 5

	Concept Paper's acknowledgement that "low impact" means that "the loss of confidentiality, integrity, or availability would not be expected to affect the BES Functions it supports" (page 19, lines 31-32), it should be clarified that BES subsystems with a "low" impact should not be subjected to regulation of cyber protection. Imposition of even limited regulation of cyber protection would impose unjustified burdens from a registered entity compliance and Regional Entity monitoring perspective. As described at page 15 of the Concept Paper, this assessment "is based on their impact on the reliability or operability of the BES, as defined by the characteristics of an ALR." As demonstrated in response to Question 1, this ALR-based test is over-inclusive and goes far beyond Section 215's purpose for reliability standards, including those for cyber security, as necessary for "reliable operations" –avoiding instability, uncontrolled separation, and cascading outages. See FPA Section 215(a)(3) and (4). Thus, TAPS' comments (in response to Question 1) about narrowing the focus consistent with the statutory security-focused directive apply to assessing impacts. There are many BES facilities and supporting cyber systems the sudden disturbance (due to cyber attack or otherwise) of which would have little or no impact on avoiding instability, uncontrolled separation, and cascading outages, and which should therefore be excluded from the scope of cyber-security protection requirements. Therefore, TAPS alternatively proposes a simpler two-tiered approach focused on the definition of reliability in FPA Section 215, based not on BES Subsystems, but on cyber systems themselves. Tier 1 would be regulated by the standards and would be directed at fortifying the cyber systems that, if maliciously used, could cause instability, uncontrolled separation, and cascading outages. Tier 2 would be all other cyber systems which would not be regulated by the standard, because their malicious use could not result in instability, uncontrolled separation, or cascading outages. This, we believe, was the original intent of the standard, to regulate the cyber security of "critical" cyber systems. Especially if NERC adheres to the inappropriate use of the ALR test for identification of BES Functions and BES Subsystems, it will be sweeping in nearly all BES facilities and the cyber systems that support them, even if they have minimal or no impact on BES reliability or security—*i.e.*, avoiding instability, uncontrolled separation, and cascading outages—if subject to a cyber attack. An additional category of "minimal" should be added to capture those cyber security assets that do not need to be covered by any NERC cyber standard, *e.g.*, the RTU communicating between a 20 MW gas turbine generator and a small utility that operates it. In particular, a cyber system that receives information but does not communicate information to those controlling the grid and does not control the operation of BES generation or transmission certainly does not need to be regulated by NERC cyber standards. Treating such a cyber system as "low impact" and apparently meriting some regulation of cyber protection would needlessly saddle consumers with unnecessary costs of regulation of cyber protection systems, and burden Regional Entities with unnecessary compliance monitoring, without in any way advancing the objective of making our grid better protected against cyber attacks, much less those that could cause the instability, uncontrolled separation, and cascading outages at which Section 215 expressly intended reliability standards to be directed. Further, cyber security assets supporting BES assets that have a minimal, if any, impact on security should not be deemed to have even a low impact for cyber purposes just because they communicate with cyber systems that *are* important to protect the grid against cascading outage, separation, or instability in the event of a cyber attack. As discussed above, with reference to the online banking example, what is key is protecting from cyber attack the systems that matter from a system security perspective, rather than putting armor on every computer that interfaces with such cyber systems or otherwise has any contribution to keeping the lights on anywhere. The Concept Paper seems to recognize that issue (Page 29, line 25) without

Question 5

	defining the "Alpha" and "Beta" companies and thereby clearly making it the responsibility of the utilities with cyber systems critical to maintaining system security (*i.e.*, avoiding instability, uncontrolled separation, and cascading outages) to mitigate the impact of interconnection with others.
GWA	Three levels of impact may be sufficient. It is important to have a well-documented process and criteria for determining whether impact is High, Medium, of Low. Otherwise, this approach will lead to confusion and inconsistent application. (See further comments in next question.)
MISO	From the wording of the Medium and Low impact descriptions, it appears these categories have little or no impact on BES reliability. Thus, two categories seem appropriate: critical and non-critical.
SCEG	We believe the concept of three levels is sufficient with the push towards NIST standards the HIGH, MEDIUM, and LOW levels would be easily integrated. SP-800-53 and FIPS 199
RFC-CIP	An Impact Level designation should be considered for the impact potential that is introduced when Subsystems and Cyber Systems used for testing, trouble shooting, and maintenance are used.
GEEI	Three is sufficient, assuming that there is not an exponential increase in cost/complexity when moving form Medium to High. Based on the reading of this document, there are more opportunities for a BES subsystem to be classified as "High" than any other ratings. If the application of security controls does not follow a roughly linear progression through Low to Medium to High, then there is little value. This will depend on what the required controls from the library of controls looks like when they are applied to each impact level. If every impact level results in the application of the same set of controls, then there is little value having the impact levels determine the controls. For example, if when mapping, it starts to look like this: Low: Password Protected, Logging, Periodic Audits Medium: Password Protected, Logging, Periodic Audits High: Password Protected, Logging, Periodic Audits, Intrusion Detection If the controls are the same, there is no need to define the different levels. It devolves into the same binary "critical/not critical" that exists today.

Question 5

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	There is not enough description for the impact levels ("high", "medium", or "low") for the MRO NSRS to make a judgment on whether it's appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - critical or non-critical.
MEC	Two classifications, critical and non-critical, are adequate. Additional levels would only add complexity. If an additional level is necessary, it would be to add a "no impact" level.
PSEG	High, Medium, and Low are appropriate levels
MMPA	As written the level of impact appears to assume that everything has the potential to impact the BES. Either the "pre-defined criteria" needs to ensure that systems which would not impact the BES are exempt from unnecessary security measures or the levels of impact need to include a level below "low" such as minimal.
SCE	N/A – see comment to question 1.
APPA	There should be an additional "de minimus" category for BES Subsystems that are so small or localized in impact that they effectively cannot contribute to a cascading outage unless there is a common mode fault affecting hundreds of such facilities. See discussion under Q6.
PAC	While PacifiCorp has concerns with the drafting team's concept of Impact Mapping it does feel that three impact levels are sufficient. Additional levels would only add confusion.
USBR	No. The text does provide sufficient clarity on the exact determination of the level. The mapping must be clear in order to be measurable. The impact determination needs to also be repeatable. It is not clear what value grading the impacts will have other than for creating severity levels.
BRAZOS	The impact levels should also include a Critical level (above High) and a None level (below Low).

Question 5

FPL	We believe that it's not the number of impact levels that's important, but rather how they are defined. In the example provided, high, medium, and low impact levels should be clearly defined. Once the definitions are provided, each entity will be able to consistently apply it in their risk assessment.

Question 6

6. Section E, Impact Mapping of BES Subsystems: Do you prefer discrete thresholds or performance based criteria for mapping the BES subsystems (e.g. MW values as opposed to percentage of total generation)?. Please explain.

Name	Comment
CLPUD	Discrete thresholds.
TNSK	Whichever method best supports the reliability of the BES is preferred. We could use percentage of total generation, but the total generation data would have to come real time from the Regional Coordinator to the Generator Owner / Generator Operator.
XCEL	Performance-based metrics are preferred as they will allow entities to evaluate assets with respect to their regional control areas
DOM	It needs to be more performance based to allow for operational differences within the regions. (Percentage of total generation is also a discrete threshold.)
FMPA	See FMPA's responses to Questions 1, 2, 4 and 5. FMPA believes that discrete thresholds are appropriate, and not percentages. The purpose of the standards as laid out in FPA Section 215 is to avoid "instability, uncontrolled separation, or cascading failure". Therefore, threats (which as described previously, FMPA believes is a more appropriate concept than BES subsystems) ought to be measured against the ability to cause "instability, uncontrolled separation, or cascading failure". Using a loss of demand threat as an example, loss of 20% of a 20,000 MW utility is a serious threat, loss of 20% of a 50 MW utility is not; hence, a discrete number such as loss of demand equal to the Contingency Reserve or equal to the largest loss of source may be appropriate.
SWPA	We prefer a combination of both. Due to the complex nature of the BES it will be difficult to apply a threshold on a continent wide basis. This is not a "one size fits all" approach; it depends on how it is configured. Each region should already have engineering based planning and operational processes in place to identify how the loss of a BES facility impacts the region. So let the regions use their information and experience to decide what the criteria should be.

Question 6

GTC	GTC prefers discrete thresholds for mapping BES subsystems. This method places the resources and investment in meeting the CIP standards on the protection of the systems rather than on the justification of the impact of the asset itself. This method is also straightforward to audit and reduces confusion. Another benefit of discrete thresholds is that assets do not dynamically change impact levels and entities can plan for the protection of systems based on their design.
DYONYX	This approach will create a mountain of clarifications, exceptions, and a complex array of decision making criteria that will be extremely difficult to resolve, design, implement and audit. Why are we creating this complex process, scales, etc. just to come down to a Low, Medium, and High concept based on a "business systems" perspective? The categorization process will become so complex that it will be difficult to determine and audit.
BPA	More clarification needed, especially on what is meant by performance based criteria. Because BPA deals more with transmission than generation, we would like clarification on how this question would apply. BPA prefers performance based criteria because discrete thresholds don't work for all conditions. For example the BES definition of everything 100kV and above. There may be some 100kV systems that are very important to the interconnected system but they are few and far between, so having a performance based criteria that allowed for indentifying the important ones instead of a blanket threshold would actually increase reliability because we could focus on a subset instead of everything. Casting a larger net only catches more fish if you are fishing where there are fish. Page 16, lines 20-25, "work in defining the detailed criteria and categorization levels for mapping of BES subsystems is underway by another Standards Drafting Team subgroup with expertise in BES planning and operating areas" feels important to what the concepts paper is discussing, yet it is being developed separately REFERENCE page 17, line 40 "BES mapping process is required to determine the impact on the BES". How will the information be re-aligned with the separate development?
SDGE	I prefer discrete thresholds for mapping the BES system, because I think it is simpler in the long run. Wording such as 1) any generator over xxx MW, 2) if the frequency dips to xx.x Hz, or voltage drops to x.xx pu are easier to understand without having to go through calculations or a conversion process.
GSOC	We feel that discrete thresholds are better than performance based criteria for mapping the BES subsystems. When conducting contingency analysis studies to determine the impact of an asset, the contingency analysis will establish the amount of MWs, if lost that would affect the reliability of the BES for various system conditions (Loading levels, network configuration, etc). Therefore, discrete thresholds are a better measure to determine the impact than performance based criteria. Another example a of discrete threshold is a generating asset exceeding the established BA Contingency Reserve allocation. Using performance based criteria could result in the asset flip flopping between being categorized as having a high

Question 6

	impact under certain conditions and then not being categorized as a high impact but rather as a medium or low impact.
CUSMO	We prefer a combination of both. Due to the complex nature of the BES it will be difficult to apply a threshold on a continent wide basis. This is not a "one size fits all" approach; it depends on how it is configured. Each region should already have engineering based planning and operational processes in place to identify how the loss of a BES facility impacts the region. So let the regions use their information and experience to decide what the criteria should be.
MH	MW highly preferred. If using percentages, users will always be converting to MW for clarification. With MW, each user can more easily determine priority importance of concerns competing for time and/or resources for mitigation. However, performance based criteria would assist to compensate for significant variation between regions. Any performance based criteria must be readily available to the individual Responsible Entity.
NST	We are not power engineers and therefore have no specific preference. However, our experience with industry clients suggests it might be appropriate to build some flexibility into defined criteria by defining multiple sets of metrics in some cases (e.g., "If MW" ≥ 'X' – or – "Pct Total Generation" ≥ 'Y' Then,…).
NPCC	We prefer performance based because an impact based mapping of BES subsystems is superior to that of a threshold based because of a cost benefit reliability ratio. Protecting cyber assets in these BES subsystems based on MW value or some other threshold will potentially lead to unnecessary expenditures and little if any incremental benefit to securing some of these systems. The effect of compromising all BES subsystems should be assessed and documented and understood. Then an appropriate level of protection should be applied depending on the impact of the failure or compromise of that subsystem. To protect "everything" above some arbitrary threshold is not cost effective.
RFC	We prefer discrete MW values. Percentages, such as percentage of total generation could miss assets for smaller companies. Also, if percentages are based on dynamic numbers such as seasonal peak or actual generation, the determination of criticality becomes a constantly changing situation.
IRC	The criteria and thresholds should be based upon percentage values (%), not discrete values, to preclude changes necessary when the discrete values may no longer apply. There is also danger in specifying detailed technical security requirement specifications within Reliability Standards since the technology along with threats, vulnerabilities and risk are constantly moving and dynamic entities.

Question 6

AEP	Each company's assets, functions and cyber systems are different and arbitrarily setting generic thresholds or criteria may not be appropriate in all cases.
MGE	Examples of both would need to be given to the industry. Why not use both and allow the Applicable Entity to make that determination as part of the Version 3 CIP Standard. This would add to the paradigm shift that is upon us now. The Standard should not be so descriptive that we have one way to determine the Impact Mapping of BES Subsystems. The complexity of this methodology will give too much opportunity for interpretation by an Auditor. This would also allow presently identified Facilities that fall below the established criteria (sub-transmission) that do impact the BES to remain having additional protection to ensure the reliability of the BES.
WE	Depending on how the discrete thresholds or performance criteria are determined, Wisconsin Electric could work with either measurement. If thresholds are used, they should NOT be implemented on a unit basis. The responsible entity should define a fleet threshold based upon State Estimator Analysis, to ensure BES stability and reliability. Then let the responsible entity select what assets need to be selected as critical to meet this threshold. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	Performance based criteria – there are too many variables to define discrete thresholds.
SOCO	As noted in our response to Question 4, we believe that adopting pre-defined, one-size-fits-all criteria is inconsistent with FERC's recognition of the need for flexibility, which is necessary to allow for meaningful implementation. As a result, pre-defined static criteria should not be adopted for mapping BES subsystems. Provisions should be allowed for entities to make rational engineering evaluations in order to identify which facilities truly have a high, medium, or low impact on BES reliability. Failure to do so will result in significant increase in compliance costs to protect arbitrary systems and no actual improvement in reliability.
E-ON	Any thresholds should be based on impact upon BES reliability
ATC	We believe that any threshold developed by the SDT needs to be flexible enough to capture both the impact of the attack on that entity's assets along with the impact on the Bulk Electric System (BES). A small entity may not have any assets that impact the BES outside of its control but does have assets that if compromised have a severe consequence on their system. Knowing this will help any entity determine how to protect its system but only those that impact (Cause cascading or large area blackouts) the BES outside of its area should rise to the NERC compliance level.

Question 6

	Any threshold developed has to identify the outage that needs to be studied. Does an entity have to look at single element outages, multiple outages or a single event that opens all breakers in an entity's system? ATC does not support a one size fits all approach if it sets predetermined levels based on a perceived impact. We suggest that the team look at the planning standards in order to get a better understanding of a study structure.
TAPS	See responses to Questions 1, 2 and 5. TAPS believes that there is a relatively simple threshold for mapping threats that can be caused by malicious use of cyber systems, and that is whether malicious control of the cyber system can cause "instability, uncontrolled separation, and cascading outages" as reliability is defined in the FPA Section 215. Making it more complicated is burdensome to registered entities and the Regional Entities. Additionally, making it more complicated and including non-critical cyber assets would distract attention from the truly critical cyber assets and extend the time required to conduct analyses to resolve problems that could actually impact BES reliability.
GWA	GWA believes that performance-based criteria would provide a more sound approach. The diversity of the asset makeup, load requirements, and system engineering in different parts of North America would mean that discreet thresholds, while easier to apply, would potentially have different consequences for different parts of the BES. Performance-based requirements should provide for a more consistent application across the BES.
MISO	Performance based criteria is always superior. Thresholds usually are selected arbitrarily and oftentimes are set low enough to include all impacting systems but as a result include many non-impacting systems. If an engineering analysis was performed and revealed an appropriate threshold that solved the issues above, this would be satisfactory.
SCEG	Performance based criteria better encompasses the entire BES and sets the same standard for all utilities regardless of their size. A percentage also better reflects each individual company's overall impact on the BES and will result in a more comprehensive impact mapping system-wide.
RFC-CIP	The example "percentage of total generation" could mean that the same BES Subsystem could have a different level of impact on any given day. This would make compliance and auditing extremely difficult therefore discrete levels are preferred. Note that NERC's Bulk Power Event Classification Scale uses discrete levels.
GEEI	Discrete thresholds are easier to manage, but will not scale over time or with facility changes. We would suggest using performance-based criteria. A minimum MW value can indicate a normal/abnormal system rather than percent base value as it can mean anything.

Question 6

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	It would appear to be appropriate to use a discrete level to be consistent with the existing NERC Operating Reliability Events Categories and the Statement of Compliance Registry Criteria Revision 5.0.
MEC	In general, discrete thresholds would be preferred since they are easier to apply and less prone to error.
MMPA	Discreet thresholds are more easily definable. Performance based thresholds would be overly difficult in identification, compliance, and auditing.
SCE	N/A – see comment to question 1.
AWEA	Clarity in criteria is important. Characteristics need to include more than just MW size or % of total generation. Capacity value or contribution to LOLE are important generator characteristics.
APPA	I would need to see a more concrete proposal before providing a single answer. Note that percentage of total generation should be a regional or large area-based criterion, since a small BA of 300 MW could lose a major percentage of its generation, e.g., 20% or 60 MW, with no measureable impact on reliable operation of the interconnection or the region. Conversely, loss of 10% of a large BA's generation due to a cyber-security event is much more likely to have a severe impact on reliable operations. There are other criteria that could be used as well, such as a. DHS Tier I, II, and III critical assets b. Current NERC standards and Requirements with high, medium and low Violation Risk Factors c. Standards associated with emergency versus normal operations or system operations versus planning d. IROLS and SOLS e. Facility Voltage (>300 kV, >200 kV, >100 kV, plus RE identified critical facilities) f. Entity or cyber-system span of control or impact (wide area versus local) The criteria above are illustrative and should not be read as a recommendation that the SDT adopt any one of them.

Question 6

PAC	While PacifiCorp has concerns with the drafting team's concept of Impact Mapping, PacifiCorp would prefer discreet thresholds versus performance based criteria as the later is very often open to interpretation. Discreet thresholds would reduce the confusion and debates within responsible entities over impact levels.
USBR	If specific threshold are needed then they need to be absolute and repeatable. Such a threshold would be specific to the system configuration rather than loading of any one resource or asset.
PGE	PGE believes that discrete thresholds that are developed by the Regional Entity and apply across the Interconnection would provide the most clarity and direction to individual registered entities.
BRAZOS	The discrete threshold approach may initially be a good starting point realizing some form of performance based criteria can be developed after some experience with the overall process.
FPL	Neither approach works perfectly. Discrete thresholds are difficult to determine with diverse areas yet strictly looking at percentage is not correct either. Determination should be by impact i.e. Causes loss of x amount of load, causes system instability, causes voltage collapse, etc. Otherwise, we believe that a performance-based criterion more clearly addresses threats to the system and ties better with other operational and planning standards. It is important to make a distinction of whether this is more cyber-focused rather than related to power systems.
TECO	Regardless of the two approaches (discrete thresholds or performance based criteria), this needs to take into consideration of the regional differences and overall regional impact within which an entity operations. The MW values, for example, need to be based on the regional area versus the entire country.

Question 7

7. Section G, Categorization of Cyber Systems describes how an entity determines the impact a specific cyber system has on its assigned BES reliability functions. Do you agree with this process as described in the concept paper? Please explain.

Name	Comment
CLPUD	No opinion.
TNSK	Yes I agree with this. The Regional Coordinator would have to explain the use and impact of the data exchange between the Generator Owners and Generator Operators as they relate to the BES Functions to determine the impact the systems have on BES reliability functions.
XCEL	We agree with the process, but there needs to be more definition on how cyber systems are mapped to BES reliability functions (the proposed functional impact that correlates to each BES subsystem). There will need to be some standardization for the meaning of each impact category (HIGH, MEDIUM LOW) so that entities will have a uniform approach to categorizing systems.
DOM	The concept is acceptable but its implementation could be difficult. For example, a state estimator ("SE") is required for situational awareness. Inputs to the SE are from SCADA RTUs. An abnormal network topology and loading could exist where the loss of a normally inconsequential RTU could cause the SE to not solve. What testing will be required to determine if the RTU is low, medium or high impact?
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. As described in these responses, FMPA believes that a threat analysis ought to be done for each cyber asset to evaluate the magnitude of the threat.
SWPA	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of protection on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

Question 7

GTC	GTC agrees with this process with one caveat. Loss of confidentiality, integrity, and availability does not affect BES cyber systems in the same way that it affects information systems. For BES cyber systems, loss of availability and integrity are much more important than a loss of confidentiality. The categorization should reflect an appropriate weighting to these characteristics that are unique to the BES.
DYONYX	We agree that if one system has a "High" impact on one function and "Low" on another, the "High" classification should be applied. The problem is the broad level of definitions for the ALR, functions, and potentially the "to be defined" criteria. See comments for Question #1.
BPA	No. For example, even though the Asset Impact is High a supporting system may not have a high level of criticality. There needs to be options to assess the cyber impact based on high, medium, low and non-applicable no matter what the asset impact level is. Also, more clarification is needed on Figure 3. There needs to be more flexibility in assessing the cyber system's impact level. May conflict with current NERC functional model and reliability functions that we are registered for. Page 19, lines 15-25, how does this apply to cyber systems, how do Entities determine how many real-time energy controls lost or unavailable will result in a "loss or compromise to the function of the BES Subsystem it supports"? Page 19, line 40, how is security categorization being defined under this concept?
SDGE	The three categories of impact (high, medium, and low) as described seem like a good process. As mentioned above, I don't think you'd want much more than three or four different categories of impact, as it would get confusing and potentially difficult to implement due to the subtle differences between a large number of categories.
GSOC	The process as described is acceptable
CUSMO	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level, the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of protection on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

Question 7

MH	The categorization of cyber systems as written mixes impact (high and low impact) and probability (medium impact). This leads to a very confusing analysis. If the team continues to use a mix of impact and probability then more levels and better descriptions are required. Manitoba Hydro suggests that only impact be assessed using 3-4 levels. A 4 level may be required for "No Impact". Manitoba Hydro suggests that the same scale as BES subsystem and levels of impact be used for the cyber systems impact analysis. This method would make the any analysis and documentation much simpler. It would also readily accommodate integrating any common mode failures for cyber systems. Confidentiality should be removed from the impact categories or handled separately under the Target of Protection. Availability and integrity (compromise) can directly result in impact to the BES Subsystem; however, confidentiality of BES cyber systems data is normally not a concern and information about BES cyber assets on separate (collateral) cyber assets do not always require the same categorization as the BES cyber asset or subsystem. The current process would require that cyber assets used to protect confidentiality would be categorized the same as the BES Subsystem which may not lead to appropriate security controls.
NST	We do not agree with the proposal to require an entity to attempt to predict the degree of impact a BES Cyber System's loss or compromise might have on the BES reliability functions it performs or supports. We believe doing so would in many instances require the application of highly subjective judgments, thus introducing to the overall analysis a significant qualitative component that we believe the SDT is striving to avoid. Moreover, we believe that following the proposed approach would, when combined with the categorization of BES Subsystems, result in a methodology that is more complex than the one defined in the referenced FIPS-199 Standard. Under that standard, the categorization of an information system is tied directly to a previously performed categorization of the information it stores and/or processes (e.g., {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}). There is no requirement to, for example, predict the severity of impact on *information* integrity of a loss of information *system* integrity. As an alternative, we recommend that identified BES Cyber Systems be categorized based on the highest level categorization of BES Subsystems whose functions they perform or directly support. BES Cyber Systems would thus be categorized as High, Medium, or Low Impact, depending on whether their associated BES Subsystems were categorized as High, Medium, or Low. We believe this modification would simplify the overall Cyber System categorization process (it would eliminate the need for the "Final Categorization" step described in Section H) and would reduce the amount of subjective judgment required while still serving the overarching objective of protecting BES reliability and operability from cyber threats.
NPCC	Agree with section G in principle, but feel that more explanation on the use of Confidentiality – Integrity – Availability security concepts is needed.

Question 7

RFC	We agree with the process in general, but have the following suggestions: a. The language must be consistent between the levels. For example, High says "...compromise of the integrity…" while Medium uses "operational integrity". b. No mention is made of misuse of a compromised system. While the CIA principles are a good basis for this discussion, they do not go far enough in considering impact of a compromised system. The impact of misuse, whether deliberate or accidental, should be a major factor in the determination of the impact of the cyber asset on reliable operation of the BES.
IRC	Yes. This section describes the activities as that of the Responsible Entity but the focus of this paper, itself, is that the interconnection between various systems and with other entities presents significant security risk. This is as true for the cyber assets as it is for the power lines. The very words listed in the Introduction support this view: "The Bulk Electric System is controlled (not the wires, transformers, relays, meters, etc…) but the highly interconnected, integrated into a single multi-state spanning machine, as vulnerable as its weakest component." The focus of the current CIP Standards is hardware focused—virtually all Critical Assets within the BES are pieces of hardware, generators and substation components and essential supporting cyber assets which are focused on specific hardware devices and components of the BES, not systems. The essential control systems needed for RC/BA/TOP functions are implied by the current CIP Standards but not specifically addressed other than from the hardware perspective. An Electric Sector organization, such as an ISO, which functions as RC/BA/TOP but which has no real hardware-based Critical Facilities or Assets has only the Control Center and it's supporting Data Center as CAs, which do not easily conform to the current risk-based approach for identifying Critical Assets. The updated standards must continue to meet the needs for owner/operators as well as for other entities such as the ISO/RTOs who have Control Centers and very large Data Centers (1500+ servers) along with the trained IT staff and system operators. As a natural corollary, our primary cyber assets are the software systems that support the Control Center operators; therefore, much of the requirements in the current CIP Standards do not apply or are distorted when applied to a fully functional data centric model. Since the subset of software centric Control Centers is a very small portion of the BES, it is recommended that an alternative approach would break out these security controls and use standard security models (ISO-27002, NIST SP 800-53 R3 or ISO pubs) to develop a security organization framework. In some instances these documents are insufficiently comprehensive to meet the ISO's needs (for example there is no NIST guideline for Windows 2003 or 2008) which could present gap in security management within the framework of the BES.
AEP	In Section G, the categorization of cyber system impacts identifies a categorization of 'low' if the loss ... 'would not be expected

Question 7

	to affect the BES functions it supports.' We interpret this to mean that regardless of the BES functions supported, there is no concern with the loss of the supporting cyber systems. Yet in Section H, Table 2 shows in the bottom row, which corresponds to a cyber system impact of 'low', but with 'final categorizations' of H (high), M (medium), or L (low), depending on the impact mapping of the BES Subsystem. It seems logical that this bottom row would be all L (low). Otherwise, more extensive and costly cyber controls than necessary may be applied. AEP contends that this categorization process will be a significant administrative burden that will not yield corresponding benefits, and could divert staff from meaningful reliability and/or security duties.
MGE	No. Once again the BES Reliability Functions have yet to be determined.
WE	Wisconsin Electric could support the categorization process. There should be additional information or examples of what loss of confidentiality, integrity and availability is and how it impacts the BES subsystem for each category of impact. This concept can be confusing to the regional entity applying the matrix. There could be cyber systems that by themselves are critical to a process but not to the overall viability of the BES or systems supporting them. These systems should not be elevated to a high status because of this fact. Again, an asset based approach would make more sense. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	We do agree with the approach, but believe the process is not clearly enough defined. Section G does not explain how definitions of Asset Impact levels (High, Medium, Low) differ from definitions of Cyber Impact Levels of High, Medium and Low. It is not clear if Asset Impact is meant to represent a likelihood of occurrence (of availability and integrity loss) or actual impact of such occurrence. It is not clear what the difference between High and Medium is other than the word "unlikely", which is very subjective. It should also take into consideration an additional "negligible" category that was proposed in question 5. In addition, loss of confidentiality should not be included in the consideration of the impact – it should be limited to loss of integrity and availability.
SOCO	Yes, we agree with the concept along with the changes described herein.
E-ON	Medium and low risks are irrelevant. Only cyber systems the loss of which could lead to instability, uncontrolled separation, or cascading failures of the BES, or impair the ability to restore BES operation, matter. Introducing gradations of risk does nothing to lessen the compliance uncertainty that exists today and invites further uncertainty as to which set of requirements app

Question 7

ATC	ATC believes that this section needs some additional clarity. It's our understanding that entities will have to first identify the "High", "Medium" and "Low" Cyber Systems which form the center of protection in the Target of Protection figure (See Figure 6 Yellow area). Along side the center of protection are three different cyber system identifiers: "Interconnected Cyber Systems", "Infrastructure Cyber Systems" and Collateral Cyber Systems" (See Figure 6). So is the team proposing additional cyber and physical protection for each of the three different cyber systems and will they be the same no matter what the center of protection category? (Example: If you have a BES Cyber System that is "High" will the different cyber systems (aka: "Interconnected Cyber Systems", "Infrastructure Cyber Systems" and Collateral Cyber Systems") have the same compliance obligations as a BES Cyber System identified as "Low"?)
TAPS	See responses to Questions 1, 2 and 5.
GWA	In general, yes, but this is associated with question 5. If there are further gradations (more than 3), consider including as part of the impact criteria, factors such as recovery time (short, medium, long – with long being 24 hours or longer, medium being a range of hours, and short being minutes to ??); and availability of alternative approaches to support reliability if a system were compromised (e.g., manual controls).
MISO	We do not agree with the assessment. Medium and Low categories appear to describe impacts that may not impact the BES. If the BES is not impacted, the CIP standards should not apply to the Cyber System.
SCEG	General Comment: Nowhere in the document is a requirement for a Cyber Security Assessment Team? Level of knowledge to perform a valid assessment/analysis would require input from various disciplines for determination of the remaining Sections.
RFC-CIP	See comment for Q5. Impact category for equipment used on an intermittent bases (i.e. test equipment) should be considered.
GEEI	The process is agreed with, but in practical application this will not be a simple determination. Systems are dependent on each other, share data, and rely on the integrity of the overall data stream. If a downstream system is classified as "Low", but that downstream system feeds data to a system that is classified as "High", then the system has been inadequately protected. The paper recognizes this, and says that the downstream system must be classified as "High". To continue that reasoning, with system interdependence constantly increasing, this will eventually lead to all systems providing some piece of data that is fed to a "High" classified system, leading all downstream systems to inherit the "High" classification, which again, devolves into the same binary "critical/not-critical" that exists today.

Question 7

LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	There is not enough description for the impact levels ("high", "medium", or "low") for the MRO NSRS to make a judgment on whether it's appropriate or not. No matter what categories are developed there should be a category with a clear distinction between assets that are considered critical or not. With the implication that the facilities deemed critical will receive a prescribed level of security. MRO NSRS believes the existing two classifications are sufficient - critical or non-critical.
MEC	No. It is unclear what value is added by having multiple classifications versus a "critical" or "non-critical" approach. The standard should be kept as simple as possible to achieve the desired goal. CIP-002 R3.1 through R3.3 list the characteristics that qualify a Cyber Asset for identification as a Critical Cyber Asset. These characteristics address a threat based on the asset's cyber accessibility (routable protocol or dial up). The characteristics of routable protocol and dial up accessibility are missing in the concept paper. They are essential to determining the impact of a specific cyber asset or system on the BES and should be included.
SCE	N/A – see comment to question 1.
APPA	The approach appears to be conceptually sound, although the definitions appear without much prior discussion of the terms used in the definitions of High, Medium or Low, e.g., "High if the loss of confidentiality, integrity, or availability directly causes or contributes to the loss or compromise of the integrity or availability of the BES Function it supports." See discussion above and consider adding a de minimus impact category.
PAC	No. It is unclear what value is added by having multiple classifications versus a "critical" or "non-critical" approach. The standard should be kept as simple as possible to achieve the desired goal. CIP-002 R3.1 through R3.3 lists the characteristics that qualify a Cyber Asset for identification as a Critical Cyber Asset. These characteristics address if there is a threat based on the asset's cyber accessibility (routable protocol or dial up). The characteristics of routable protocol and dial up accessibility are missing in the concept paper. They are essential to determining the impact of a specific cyber asset or system on the BES and should be included.
USBR	No. The impacts described are very subjective. Most of the definitions as written can only be described through statistical analysis. Language such as "contribute" or "compromise" does not lend itself to factual assessment rather to judgment. The impact on the BES is best determined by the Registered entity based on function of the critical asset and its relation to the

Question 7

	BES.
PGE	The categorization of cyber assets based on the impact of the system that they are involved in could lead to confusion if multiple assets of different impact levels are included within the same environment. Instead of having a clear line of demarcation for what is and is not under CIP control, as in the current framework, this approach presents an additional compliance and security risk as assets that are housed in the same physical environment are subject to very different sets of controls. This mixed environment could lead to avoidable human error because someone mishandles a system.
FPL	We agree with the methodology as it is based on impact, however, we believe that the process as described is not as well defined and can cause confusion resulting in unnecessary systems as being identified as critical when they do not have significant impact to the BES.
TECO	We agree in principle with the approach; however, we believe that the process to develop and maintain this list is going to be very complex and will take significant education, knowledge, and awareness to complete/maintain.

Question 8

8. Section H, Final Categorization of Cyber Systems Based on Overall Impact on the BES describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a cyber system has on the BES. Do you agree with this process described in the concept paper? Please explain.

Name	Comment
CLPUD	Central Lincoln sees no way a low impact asset could correspond to a high cyber impact on the related cyber asset. The reverse, however, might occur. Suggest removing the elements above the diagonal on Table 2.
TNSK	Yes, this is a good process.
XCEL	We agree with the overall approach, but there needs to be additional detail on the final categorization output (again, a standard approach to evaluating the overlap of asset and cyber impact) as well as allowances for a fourth category for cyber systems that have no impact ("NONE" or "N/A").
DOM	No. As another way to do an assessment, if the impact of a cyber system is high (that is, it supports a critical BES function), but the cyber risk is low (based on a probability of failure caused by an outside source), then we would propose the overall rating of the cyber system should be low. Low cyber system ratings would then require less constraints or less support. This follows what is understood to be one of the goals discussed on the 8/25/09 Webinar – put your resources and time on those cyber systems that have more of a chance of leading to failure. In Table 2, is the Asset Impact actually referring to the BES Subsystem Impact?
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6.
SWPA	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.

Question 8

<table>
<tr><td>GTC</td><td>GTC agrees with this process, but does not concur with the sample categorization table included in Table 2 of section H. A high water mark of BES subsystem impact and cyber system impact does not accurately reflect the impact on reliability of the BES. A more appropriate table might look like the following:
<table>
<tr><td>Asset Impact →</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Cyber Impact:</td><td></td><td></td><td></td></tr>
<tr><td>High</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Medium</td><td>Medium</td><td>Medium</td><td>Low</td></tr>
<tr><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr>
</table>
If by definition, a Low Impact Cyber System is not expected to affect the BES Function it supports (p. 19 line 31), then it should not be required to be protected at a High due to its relation to a subsystem that may in fact have impact on the BES.</td></tr>
<tr><td>DYONYX</td><td>We do not believe the deterministic methodology defined in this document will provide a consistent approach. First, the basic broad definition of ALR is not applicable to the objective herein which leads to even more confusion in the defined functions and BES Subsystems. Can we not come up with a more definitive front end process when we are looking at categorization of systems associated with impacting the operation of the BES?</td></tr>
<tr><td>BPA</td><td>Not entirely. There needs to be more clarification on the high, medium and low classifications. What is a low example? Also, a Non-applicable option needs to be added that covers systems where no action is needed. As an example, how would a utility handle a high subsystem, with a high cyber system supporting it which has no interconnectivity whatsoever?

BPA does not agree with the examples in Table 2 of section H showing a high impact for all high cyber impacts. We think the asset impact should be the overriding categorization. Thus, a low asset impact would have a low impact even if the cyber impact was high.</td></tr>
<tr><td>SDGE</td><td>At first glance, the process described in the concept paper for Final Categorization seems okay. It's difficult to comment substantively on the process, however, because the example shown doesn't have any details behind it. You know what they say, the devil's in the details. Since Table 2 is not an actual table (per the note included), it does leave me a little confused as</td></tr>
</table>

Question 8

	to what an actual table would look like.
GSOC	The process as described is acceptable
CUSMO	The process is good in that it allows for different levels of impact. However, there needs to be four levels of impact; High, Medium, Low and Not Applicable or None. Without the fourth level the current process will force all registered entities regardless of size or location to identify all of their BES subsystems and then be responsible for documenting at least a low level of impact on all of these systems. There is no exception for subsystems that have little or no impact to BES reliability. We do not agree that these systems should have to be monitored for compliance to mandatory standards and financial penalties.
MH	Manitoba Hydro does not agree with the example of overall impact on the BES. The table indicates that most cyber assets will require the same security controls associated with the HIGH category and few cyber assets will receive the LOW categorization. A mapping between impact categorization and security controls should be developed by first identifying all the necessary security control levels; then sample cyber assets should be mapped into the security controls and finally a representative table or mapping list should be documented. The security controls should provide for additional criteria such as layers of security protection including those outside the ESP or PSP, use of private communications or other private facilities with restricted access. All layers should not need to be as described in the current CIP Standards (i.e. 6 wall perimeter, etc.). Responsible Entities may have a significant investment in private communications and other security layers to improve reliability. Private communications and other layers of security should be allowed to provide part of the mandatory security; otherwise unintended consequences could result by discouraging private communications and additional layers of security controls.
NST	We believe this step can and should be eliminated by simplifying the Cyber System categorization process (see our response to Question 7, above).
NPCC	Agree with this process.
RFC	We agree. This approach would achieve the goal stated in section H of providing a more consistent approach than application of a risk-based methodology as presently required in CIP-002-1 and CIP-002-2.

Question 8

IRC	Concur that pre-determined categorization of the cyber system should be based on both the impact mapping of the supported BES Subsystem and the impact of the cyber system on the BES function it supports. Some may argue that categorization should be exclusive, i.e., that High be only selected when both functions are high, not when either of the functions is high as proposed in the concept paper; however, we disagree and concur with the approach outlined in the concept paper.
AEP	Please refer to our comments in item 7.
MGE	There should be two levels, critical and non critical. The SDT assumes that all BES Subsystems have an impact on the BES. As in the presently written CIP-002-1 methodology, a system is set up to see if an item is critical or not. This is not present in this concept paper. An example might be a 15MVA generator connected at the Distribution level, connected to SCADA/EMS and not blackstart capable. This concept paper would probably say it is in the "Low" impact category. Why? Because the Concept Paper (SDT) assumes it should be. There may be items that don't fall within this BES Subset and would be placed in the "non critical" category.
WE	Wisconsin Electric feels that additional information around standards required for compliance based on categorization level (impact mapping) along with the type of cyber system considered should be provided before answering this question in the positive. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	There needs to be a more nuanced approach to assessing the impact – any high should not automatically be high. If asset impact is high and cyber impact is low, or asset impact is low and cyber impact is high, the categorization should be medium.
SOCO	Yes, we agree with the concept along with the changes described herein.
E-ON	This deterministic methodology in comparison to the risk methodology in place today appears to radically increase the number of facilities that will be subject to NERC CIP standards. This methodology will, at minimum, necessitate more time for affected entities to verify and, if necessary, implement CIP compliance verification at far more facilities than has been the case in the past. The current 6 to 12 month period is insufficient to accomplish this undertaking.
ATC	Table 2: Page 21 ATC does not agree with the table as proposed. We believe that if this table is to be used the lower of the Asset Impact and Cyber Impact ranking should be used to determine the BES Function. (Example: If a BES Subsystem has a "Low" Asset Impact, or no impact, event then there is no benefit to treat it exactly the same a BES Subsystem that has a "High" Asset

Question 8

<table>
<tr><td></td><td>Impact just because of the Cyber Impact ranking. We believe that entities should not be expected to treat BES Functions that have little or no impact on the BES the same as BES Functions having a "High" impact because the cyber impact on the BES function. ATC does not see a reliability benefit in protecting BES Function the same if their impact on the BES is not identical. In addition if you have a BES Subsystem that is "High" but it has a cyber Impact of "Low" it should be rated "Low". The reason is that the cyber system identified as "Low" would have no affect on the BES Function so why expect the same level of protection on these different BES Functions.)

The SDT should adopt the following table if this effort is going to be pursued further:
<table>
<tr><td>Asset Impact ></td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Cyber Impact:</td><td></td><td></td><td></td></tr>
<tr><td>High</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>Medium</td><td>Medium</td><td>Medium</td><td>Low</td></tr>
<tr><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr>
</table>

ATC believes that the designation of "High", "Medium" and "Low" could be replaced with a system more like the Categorization of Events (1-5) (Page 16 of the concept paper). Since the Categorization of Events was suggested as a possible input into the impact assessment if the 1-5 is not adopted, then how will the SDT place the events into the "High", "Medium" and "Low" categories. (What would be the process to move the 5 Categories of Events into the three categories suggested by the SDT?)

The SDT needs to present their thoughts on the compliance obligations for whatever categories they determine are appropriate. The determination of the compliance obligations for each category is the cornerstone to this whole effort and if not supported by the industry could result in a drastic delay in addressing actual FERC directives.

ATC believes that if this table is used additional compliance obligations should only be placed on BES Functions that fall into the "High" box. Medium and Low BES Functions could be identified but should not be subject to additional compliance obligations.</td></tr>
<tr><td>TAPS</td><td>See responses to Questions 1, 2 and 5.</td></tr>
<tr><td>GWA</td><td>Yes.</td></tr>
</table>

Question 8

MISO	The impact on the asset is all that matters. The purpose is to protect the BES. If a cyber system is compromised but has no impact on the BES that cyber system is not even relevant to reliability. If a cyber system has a high impact on a BES element but the BES element has a low impact, the BES is not likely to be compromised because the actual BES element has a low impact.
SCEG	Consideration should be given as to how the newly classified "cyber systems" will fall under CIP-003-CIP-009 since these standards currently address a more narrow scope of cyber assets. This new apporach will result in many more cyber systems (and targets of protection) being identified, and the result may bring undue burden on utilities and/or require infeasible application of the additional CIP-003 through CIP-009 standards. Consideration of each category of cyber systems should be analyzed to determine the feasibility of implementing the remaining CIP standards. In other words, the applicability of the remaining CIP standards should be based on the "type" of Target of Protection or various exemptions should be allowed.
GEEI	Agreed, this is generally no different than the current risk-based assessment, except that two of the key variables that are inputs to the overall risk assessment have been defined by a fixed process through the impact mappings. The matrix should show the 3 characteristics, availability, integrity and confidentiality as variables for asset impact and cyber impact.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No. It will result in a mis-allocation of resources to highly improbable or impossible events. The approach adds complexity without providing a reliability benefit. Misallocation of resources will decrease the reliability and safety of the BES creditable threats both cyber or non-cyber will not receive sufficient resources given that there are finite resources to allocate.
MEC	No. The overall approach adds several layers of complexity and it is unclear if it would produce improved results. MidAmerican is concerned with the complexity in the process proposed, questions if the process is repeatable on an annual basis and challenges the resulting security categorizations. As defined by ISO/IEC Guide 73, risk is the combination of the probability of an event and its consequence. The proposed categorization addresses only impacts (consequences) but does not address probability. As a result, how can the final security categorizations accurately reflect the risk posed by the Cyber Asset and what security measures should be applied? The proposed approach does not provide more clarity than providing more specific criteria for asset selection under the current approach in the standards. More specific details would be required under any approach. Adding clarity and specificity to the current standard is more productive. MidAmerican's methodology yielded rational results within the standard's current framework without multiple classification levels

Question 8

<table>
<tr><td>SCE</td><td>N/A – see comment to question 1.</td></tr>
<tr><td>AWEA</td><td>Based on Table 2 the process is either unclear or flawed. If a cyber system has a Low impact ("not expected to affect the BES Function it supports") why would the Final Categorization ever be rated as High regardless of the Asset Impact? Iron clad cyber protection of that cyber system would still have no impact on BES reliability.</td></tr>
<tr><td>APPA</td><td>Yes, but with all of the misgivings identified above. My primary concern is that the resulting deterministic matrix implies a level of categorical precision that does not exist in practice. This concern is not obviated by the statement that the evaluation matrix in Table 2 on page 21 is illustrative. That being said, current CIP-002 implicitly has a four cell matrix.</td></tr>
<tr><td>PAC</td><td>No. PacifiCorp feels the same results could be realized using only two categories of critical and non-critical. The overall approach adds several layers of complexity and it is unclear if it would produce improved results. An example is provided below:
<table>
<tr><td></td><td colspan="3">Asset Impact</td></tr>
<tr><td>Cyber Impact</td><td>High</td><td>Medium</td><td>Low</td></tr>
<tr><td>High</td><td>Critical</td><td>Critical</td><td>Non-Critical</td></tr>
<tr><td>Medium</td><td>Critical</td><td>Non-Critical</td><td>Non-Critical</td></tr>
<tr><td>Low</td><td>Non-Critical</td><td>Non-Critical</td><td>Non-Critical</td></tr>
</table></td></tr>
<tr><td>USBR</td><td>No. If the original thesis is examined under which we are trying to protect our cyber assets categorizing something low still results in an impact and may reveal a exploitable vulnerability.</td></tr>
<tr><td>PGE</td><td>PGE does agree with this process and believes that it would produce consistent results.</td></tr>
<tr><td>FPL</td><td>We agree with the process as described, but believe there is still a need for risk-based assessment to be performed.</td></tr>
<tr><td>TECO</td><td>We agree in principle with the approach; however, we believe that the process to develop and maintain this list is going to be very complex and will take significant education, knowledge, and awareness to complete/maintain.</td></tr>
</table>

Question 9

9. Section I, Defining the Target of Protection describes how an entity determines the set of cyber assets necessary to provide security assurance in the BES functions the cyber system performs. Do you agree with this process described in the concept paper? Please explain.

Name	Comment
CLPUD	It is unclear what the goal is here. Will the non-BES cyber assets be required to meet CIP-003-009?
TNSK	This is flexible, but is silent on the risk of attack, for example whether or not the protocol is routable or non-routable protocol, or if the system is properly isolated.
XCEL	We agree with the overall approach, but the paper's definitions require additional clarification. There also needs to be agreement on how 3rd party systems are addressed and who is responsible for communications links between systems and assets.
DOM	In general, this concept is agreeable. The flexibility for the owner to define a Target of Protection is appreciated. The concept of Collateral Cyber Systems is also agreeable, but it may not always be practical to move it out of the Interconnected or Infrastructure network segments. There are concerns about the inclusion of communication links within a Target of Protection. Specifically, communication links have always been excluded because there may not be a practical way (or identified need) to protect them. It is also appreciated that Section I uses the Target of Protection concept to identify more standard cyber components. On line 32 of page 23 it identifies devices such as routers, switches, firewalls, etc., as the actual components supporting cyber systems. It would have been better to develop this concept more in the beginning of the paper rather than emphasizing BES components, because this would seem to be the ultimate targets to be analyzed and protected. Also, the paper never seems to fully develop how the Target of Protection will be linked with the rest of the concepts presented in the paper or with the existing CIP standards themselves. This subject needs to be more fully developed.
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. While FMPA agrees that cyber systems ought to be separated by where security is administered, e.g., unsecured connections between components of a system are part of the same system, we do not think that we need to define a new term "Target of Protection" but rather more succinctly define cyber systems as those systems whose boundaries are determined by where cyber and/or physical security is administered. If neither is administered, then there is no boundary. For instance, a substation automation scheme that interconnects all of the digital relays in a

Question 9

	substation without cyber (e.g., firewalls) and/or physical (e.g., the relays are not connected together in a system – air gap) security would be one system. Alternatively, if there is a substation automation scheme where the relays are only connected through cyber security protocols in a "star" arrangement, then each relay would be a separate cyber system, and the central processing of the substation automation would be a separate cyber system. If loss of the substation could cause "instability, uncontrolled separation, or cascading failure", then the central processing of the substation automation could be a critical cyber asset regulated by the standards – including the cyber security protecting the connection between the relays and the substation automation processing; whereas individual relays may not be critical cyber assets depending on whether control of a relay could cause "instability, uncontrolled separation, or cascading failure".
SWPA	Yes, it appears to give us more flexibility than the current approach.
GTC	This section needs significant clarification. The approach appears acceptable from a theoretical viewpoint, but actually implementing this process is not practical.
DYONYX	Our understanding is that BES Cyber Systems would be protected in the same manner as Critical Cyber Assets in the current paradigm. However, protecting BES and non-BES Cyber Systems that in turn protect BES Cyber Systems, and including the same in the Target of Protection perimeter, is quite an extension to the original intent and scope of the Standard. Adding an additional layer of systems, utilizing different controls, is going to just mindboggling. In addition, nothing has been said about routable versus non-routable protocols. Section J notes that "external party dependencies cannot be ignored". This technically sounds good but, in our opinion, this will be a monster to design, implement, and sustain.
BPA	We felt that this assumes the utility has a combined IT and field network, which BPA does not. The figures in this section may not apply directly to cases where there is operational system isolation. Also, clarification is needed on the term Collateral – proximity in terms of physical location or network? No option to exclude a system that may touch the BES. Need ability to assign "N/A" Note, there are many terms not well defined to be able to adequately answer this question. Page 23, lines 15-20, what is "target of protection? Page 23, lines 20-25, discuss historical data collectors (think PI), "ICCP nodes, operations support workstations, etc" appears we must now consider that which we had already excluded from our critical cyber assets lists Page 24, figure 5, no workstations are listed in the "BES Cyber Systems" circle

Question 9

	Page 25, figure 6, HMI (human machine interface) listed in the "BES Cyber Systems" circle; appears contradictory to figure 5 on page 24 Page 27, lines 5-10, what is the definition of "network proximity"?
SDGE	This section is a little easier to understand because there some additional real-world examples shown. I'm agreeable with the process as shown. One comment gathered from others in the company regarding the Target of Protection: It's obvious that the Target of Protection as defined will consist of a much wider footprint than what the current CIP Standards require, especially in the area of substations. Aside from the increased cost to implement these new protections, colleagues are concerned about the potential implementation schedule for these requirements imposed by the wider Target of Protection. To be realistic, these will probably double the size of our current CIP efforts, which is a substantial amount of additional work. We're all for Cyber Security and are supportive of the CIP Standards, there are just some internal concerns about the implementation schedule and how we manage the increased requirements.
GSOC	Section I, is confusing making it difficult to agree or disagree. Rewording and adding more clarity might help eliminate confusion. May consider adding a table or incorporate into Table 1 General comment: In the circle diagram for Control Centers the Interconnected Cyber Systems section has a PI Server, this should be changed to Data Historian Server since PI is an actual product name and this document should be product neutral.
BGE	This section indirectly redefines the Electronic Perimeter for CIP, by broadening the scope of the perimeter. The too broad definition of "Target of Protection" is making almost all of the enterprise IT systems (if they are on same corporate network) Critical Cyber assets. The concept described in this section can be applied to pure electric systems such as SCADA easily, but it is very difficult (or almost impractical) to implement this to AMI Systems which connect to corporate IT Systems (e.g. Meter Data Management System, Single sign-on Servers), electric devices such as advanced meters and AMI communication network which could be built on a public network. This concept is also difficult to implement on a Load Management system where it too connects to corporate IT systems such as the Customer Information System, GIS, Load Settlement and Customer Self Serve. In addition many load management systems are built on public paging systems utilizing one way communications.
CUSMO	Yes, it appears to give us more flexibility than the current approach.
MH	The Target of Protection to determine the cyber assets necessary for security is quite extensive and complete.

Question 9

	Identifying the target of protection should be performed prior to categorization of the cyber assets. In this manner, the impact of these other cyber systems can be individually identified including their loss or compromise. This should lead to a more thorough analysis and better mapping to the appropriate security controls. The interconnectedness and inter-dependencies can also be included in the analysis. Technologies which provide effective air gaps should be permitted to reduce the impact of interconnected cyber systems.
NST	We agree with the basic concept of defining a "Target of Protection" that considers both identified BES Cyber Systems and cyber systems with which they interact or on which they depend. However, we also suggest the following changes: • We recommend renaming "Interconnected Cyber Systems" to something that (1) more clearly indicates their indirect involvement in or support of BES functions and (2) distinguishes them from other types of cyber systems within a "Target of Protection," many or all of which may be logically interconnected with BES Cyber Systems. Suggested examples are "Ancillary BES Cyber Systems" or "Secondary BES Cyber Systems." Were the SDT to adopt this recommendation, it might then also consider renaming, "BES Cyber Systems" to "Primary BES Cyber Systems," thereby indicating their direct performance or support of BES functions. • We recognize that a given Responsible Entity's BES Cyber Systems may very well interact with and/or depend on "Interconnected Cyber Systems" that are owned and/or operated by third-parties. However, we believe that assuring such third-party systems have appropriate security controls is a very different problem than assuring one's own cyber systems are properly secure,* so we recommend that third-party Interconnected Cyber Systems be identified separately from Entity-owned Interconnected Systems. * We believe, in fact, that unless Entities are given the means to exert some degree of control over how third-party cyber systems are protected, they will consistently define Targets of Protection that do not include any third-party systems. See our comments on Section J ("External Cyber Systems") below. • We recommend the SDT identify cyber systems described on Page 23 Lines 29-33 (routers, switches, etc.) as "Infrastructure Cyber Systems," as is done in Figures 5 and 6. • We suggest revising the paragraph defining "Collateral Cyber Systems" to either (1) remove implementation recommendations or (2) allow the *option* of applying the same or possibly a modified set of security controls to Collateral Cyber Systems as those applied to BES Cyber Systems instead of moving Collateral systems to a different network segment (which might be difficult and/or costly in some cases). This would be consistent with how non-critical Cyber Assets within an Electronic Security Perimeter are handled under the current version of CIP-007. • The paragraphs and figures on Pages 27 and 28 seem to suggest a one-to-one equivalence between "Target of Protection" and "Electronic Security Perimeter" but are somewhat unclear. We recommend that the SDT concentrate for now on identifying Targets of Protection and defer discussions of what various approaches to grouping Cyber Systems

Question 9

	within one or more Targets of Protection might mean from a logical and/or physical security standpoint, lest such discussions become a distraction.
NPCC	Agree with this process, but struggled understanding the correlation between the text and diagrams.
RFC	We agree. The approach described in Section I provides a better approach to identifying the additional cyber systems that need to be protected, as well as those non-critical or collateral systems that a entity may wish to remove from the target of protection.
IRC	Yes. We especially appreciate the breakdown in the TOP that demonstrates how this might work for Control Centers, as well as Gen/Transmission facilities. We look forward to reviewing the next level as the SDT moves forward
AEP	The inclusion of supporting systems (i.e. environmental controls and monitoring systems) and the "Collateral Cyber Systems" could exponentially increase the assets in scope and complexity without any commensurate gain to security or reliability of the BES. In addition, Section J describes the interconnection of external cyber systems. It is unclear how an entity can assume all of the risks associated with an external entity's systems and the data connection (which might be a leased communication line from an independent provider).
WE	While Wisconsin Electric can agree in concept to this process, we feel additional definition should be presented around how various cyber systems would be treated based on high, medium and low categorizations. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	This is difficult to answer because the concept is not clearly defined. The systems suggested to be part of the *Target of Protection* population would seem to considerably expand the existing regulatory compliance scope of the affected utilities thus residing in higher compliance costs for the industry.
SOCO	Additional information is necessary to adequately access the impact.
E-ON	The concept paper's "Target of Protection" appears a roundabout way of stating that equipment connected with a BES cyber system so as to create the potential for communications access to the BES cyber system requires protection. The concept

Question 9

	paper also does not limit this concern to networks employing a routable protocol as is the case today and as is appropriate
ATC	The concept paper is not clear if the other categories "Interconnected Cyber System", "Infrastructure Cyber System" and "Collateral Cyber System" will be treated the same for each of the three categories (High, Medium and Low) for BES Cyber System.
TAPS	See responses to Questions 1, 2 and 5.
GWA	The description in Section I is helpful.
SCEG	The Concept looks good in paper, but the reality would be many of the Collateral Cyber Systems will be more integrated. This will make the removal of the systems a greater challenge
GEEI	The *concept* isn't disagreed with, but security is not generally as simple as: "choose system/function from column A, impact from column B, and security requirements show up in column C". It is a laudable goal to pursue this table, but far too often the answer depends on factors that are not easily quantified. Collateral systems which have impact on other regulations i.e EPA, need to be considered.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	No – MRO NSRS believes the concepts presented in the paper could cause significant scope creep resulting in the addition of components that previously were not required to be included, or were deemed non-critical given their limited or no impact onto the reliability of the BES.
MEC	No. MidAmerican agrees with a Responsible Entity having flexibility in defining a Target of Protection to maximize efficiency in secure operations. MidAmerican accomplished this by analyzing the Cyber Assets without the additional proposed layers of complexity of cyber system grouping and labeling. Additional specificity would be needed for all entities to achieve consistency. Section I introductions potential significant scope expansion by adding "non-BES Cyber Systems." MidAmerican agrees with Section I's conclusion that unnecessary Cyber Assets should be moved out of the other protected network segment. This can be accomplished within the existing standards' framework and without additional layers of process complexity. MidAmerican generally agrees with figures 5 through 7. Figure 8 and figure 9 are unclear and could be construed to expand

Question 9

	scope to include communication links that are explicitly out of scope in the current standard. Section J discusses interconnections and information exchanges across multiple organizations. It is unclear what is meant by "a third party data connection outside of the traditional Electronic Security Perimeter" or what is intended (beyond what is already achievable in the existing standards) by "the responsibility to mitigate the risk" of an external interconnection.
PSEG	The term Target of Protection is capitalized but not defined in the NERC glossary, nor is there a current SAR to have the term defined and added. PSEG recommends the drafting team consider developing a clear definition of the term and take the necessary actions to have the definition added to the Glossary, or, eliminating the term altogether.
SCE	N/A – see comment to question 1.
APPA	The framework appears to be conceptually sound. Delineating the differences between BES, Interconnected, Infrastructure and Collateral Cyber Systems would appear difficult to this cyber non-expert. On page 23 at lines 29-34, an italicized definition of "Infrastructure Cyber Systems" appears to be missing.
PAC	No. While PacifiCorp agrees that a Responsible Entity should have flexibility in defining a Target of Protection to maximize efficiency in secure operations, we feel that Section I introductions potential significant scope expansion by adding "non-BES Cyber Systems." PacifiCorp agrees with Section I's conclusion that unnecessary cyber assets should be moved out the other protected network segment. This can be accomplished within the existing standards' framework without additional layers of process complexity. PacifiCorp generally agrees with figures 5 through 7. Figure 8 and figure 9 are unclear and could be construed to expand scope to include communication links that explicitly out of scope in the current standard. Section J discusses interconnections and information exchanges across multiple organizations. It is unclear what is meant by "a third party data connection outside of the traditional Electronic Security Perimeter" or what is intended (beyond what is already achievable in the existing standards) by "the responsibility to mitigate the risk" of an external interconnection.
USBR	No. The concept does not provide security assurances. The premise expounded in the concept is that any subsystem can result in a BES impact. The flaw is in the determination of the impact. A Cyber subsystem of a BES Cyber Asset may fail, however, that does necessarily mean the BES is at risk. The overall complexity of the defense against a cyber failure cannot compromise the functionality or maintainability of the cyber asset. This Target of Protection moves in that direction.

Question 9

PGE	PGE is not able to provide meaningful comment on this approach without greater understanding of the pre-defined criteria that are used to categorize Cyber Assets.
FPL	Agree with the process and find it helpful. Although its application must be left to the individual utilities, the process is still too broad and should provide clarification. In addition, clearer expectations of the systems in Figure 8 should be provided.
TECO	Section I provides a good representation of what a Registered Entity must do in order to separate the non-critical cyber assets (collateral cyber systems) from its critical cyber systems in order to improve cyber security controls in the most cost effective manner.

Question 10

10. Provide your company's thoughts on applying different levels of protection (i.e., security controls) based on characteristics and impact categories of specific BES cyber systems (e.g., transmissions substations, generating plants, control centers) as discussed in Section K, Applying Security Controls to the Target of Protection, of the concept paper.

Name	Comment
CLPUD	Seems to go well beyond the scope of CIP-002. Is this the intent?
TNSK	The impact category to a Cyber System and determination of Target of Protection for Generator Owner and Generator Operators will need to be completed with the assistance of the appropriate Regional Coordinator.
XCEL	We support the overall approach of developing different levels of protection based on characteristics and impact. However, more detail needs to be provided on what the security controls catalog contains and what will be required for implementation.
DOM	Other than basing it on having evaluated every piece of equipment, Dominion fully supports the ideas expressed in Section K. A flexible approach that "mitigate[s] risk while maximizing the value of the associated cyber security investment… without unduly requiring entities to invoke exception processes in the standards" is exactly what these standards should be about. Also, while it is understood that the ultimate goal of the standards to be developed is to protect the BES, this standard itself should concentrate on cyber components only. Referring to a substation as a BES component is confusing. A substation is not a cyber system. It is a system comprised of many components, both mechanical devices, electrical devices and cyber devices. In this paper, the Target of Protection concept needs to be concentrated on cyber systems first.
FMPA	See FMPA's responses to Questions 1, 2, 4, 5 and 6. FMPA believes there ought to be only one level of protection regulated by the standards, and only on "critical" cyber systems that can cause "instability, uncontrolled separation, or cascading failure". While entities can and will use cyber security measures on non-critical cyber systems, there is no need to regulate these security measures.
SWPA	The process is good in that it allows for different levels of protection based on impact. However, there needs to be acknowledgment that not all cyber systems necessarily impact the BES. There needs to be an exception for subsystems that have little or no impact to BES reliability.

Question 10

GTC	It is absolutely crucial to have controls appropriate to the characteristics of the environment (substation, generating plants, control centers). An unmanned substation in a rural area has different vulnerabilities than that of a data center in an office park. Controls should be applied that are appropriate to the risk profile of the system being protected.
DYONYX	We believe a two tiered set off levels is adequate. Why make it complicated and very difficult to implement and sustain? See comments to question # 1.
BPA	See answer in Comment #11 Would like clarification of terminology comment. Page 29, lines 25-30, implies that utilizes that identify a cyber system as "high", but their external interconnected partner does not take full responsibility to mitigate any risk associated with the cyber system; What does full responsibility mean here?
SDGE	The idea of applying security controls to the Cyber Systems within the Target of Protection seems reasonable. It stands to reason that different levels of protection would be proper, given the new impact categories. In our internal discussions, we talked about the library of controls that the drafting team will develop. Those seem key in determining what actual steps must be taken in the protection of our Cyber Systems. As mentioned above, the general concept presented seems okay, but there are a lot of missing details that make it difficult to comment substantively. For the limited amount of information presented, it seems workable.
GSOC	Our company agrees that different levels of protection are definitely needed and this approach will achieve that. The different environments, a Control Center, a Plant DCS or a Transmission substation will require different security controls, therefore developing a library of controls appropriate to the cyber subsystem is a good approach.
BGE	It is likely that the CIP compliance management (i.e. the paperwork) for substation cyber assets is likely to increase dramatically and encompass most BES stations, probable unnecessarily if the primary intent is to provide Adequate Levels of Reliability to the BES. Substations typically exist in more numerous, simpler, more effectively isolated, and very different cyber environments than federal government IT systems. The continued march toward increased reliance on IT- centric security standards in use by the government will be a confusing impediment to effective and easily understood implementation of cyber security measures in most substations. We ought to be able to talk in the standards about cyber security for protective relays, RTU's and other common substation equipment without obscuring that discussion with lot of language intended to apply to large data processing systems with confidential information on a WAN connected to the Internet.

Question 10

CUSMO	The process is good in that it allows for different levels of protection based on impact. However, there needs to be acknowledgment that not all cyber systems necessarily impact the BES. There needs to be an exception for subsystems that have little or no impact to BES reliability.
MH	All the categorization of BES Subsystems and Cyber Subsystems should be as simple as possible to map to the appropriate security control level. The overall process and documentation should be kept to a minimum. Flexibility for Responsible Entities to choose the appropriate impact levels will optimize the process. If the final process does not allow for flexibility then the overall process should be simplified to a chart of impacts versus required security controls.
NST	We strongly endorse the concept of developing requirements that take into account the sometimes significant differences among built-in security capabilities of various types of BES cyber systems. At the same time, however, we believe there will be instances, for example in the case of "High Impact" cyber systems, where the Standards should continue to require the application of equivalent protections using alternative controls, if necessary. We also recommend that the SDT consider allowing for different or customized levels of protection to be applied to some cyber systems and/or their constituent elements within a single Target of Protection (Section F concludes with a statement suggesting to us that all cyber systems within a Target of Protection will require the same level of protection as BES Cyber Systems within). For example, the Availability requirement for a SCADA/EMS system server might be High, while the "real-world" Availability requirement for any one of its operator workstations might be only Medium, or perhaps even Low. We believe this recommendation supports the SDT's goal of maximizing the return on industry investment in cyber security.
NPCC	We agree with applying different levels of protection if you remove from this question "(e.g., transmissions substations, generating plants, control centers)" because those are not cyber systems.
RFC	Different levels of protection based on net impact of the cyber system is an excellent idea. It tracks with most major IT governance solutions in use.
IRC	We are supportive of the approach used in NIST SP 800-53 R3 which uses a building block approach of some controls for low level risks and then increases the controls if the higher risk levels is Medium or High. We do not see the need to re-invent basics for Control Centers and supporting Data Centers. However, the Generation and Transmission organizations may be challenged by this approach, given the differences and more complexity of the security tasks facing those entities.
AEP	Any methodology for securing essential cyber systems should allow a degree of flexibility and discretion by the responsible

	entity. The methodology should provide a framework to allow the flexibility without pre-determining the set of controls that should be used.
WE	This has merit. Transmission substation control systems, generation control systems and control centers have evolved at different rates regarding internetworking technology. Relay controls do not have the same protective capabilities as more traditional windows based architectures as seen in the control center areas. This makes it difficult or impossible to deploy malware protection (antivirus) on a solid state network connected relay resulting in creation of a TFE under the current standards. This is just one example of problems we are presently encountering applying the current standards across all critical cyber assets. The protection levels should take into account the probability of occurrence (risk) as currently used in CIP 002-1. Wisconsin Electric also supports comments submitted by EEI on this subject.
DUKE	Needs to be coordinated with other groups that are trying to do the same thing, such as groups developing Smart Grid standards. We do support varying controls, similar to the NIST model - NIST standards can be applied to the *Target of Protection* to ensure industry wide consistency in adoption of existing standards.
SOCO	Different levels of protection are needed to appropriately address the variance of risks between BES cyber systems. Moreover, the connectivity and/or other vulnerabilities to outside the electronic security perimeter should be considered in determining the appropriate level of protection.
E-ON	Medium and low risks are irrelevant. Only cyber systems the loss of which would lead to instability, uncontrolled separation, or cascading failures of the BES are relevant. Introducing gradations of risk does nothing to lessen the uncertainty over compliance that exists today and invites further uncertainty as to which set of requirements apply. It should not be an undertaking of the drafting team to develop security controls or control "specifications." The drafting team should develop minimal requirements that when adhered to insure BES reliability. Affected registered entities then implement security controls that meet or exceed these requirements, and therefore further BES reliability, while maximizing the value of their own cyber systems investments
ATC	Applying different levels of protection based on asset characteristics and BES impact is a step in the right direction. However, the type and scope of the threat needs to be known. For example, if the threat is assumed to be a coordinated physical and cyber attack on multiple assets, systems and facilities, the level of protection would be vastly different then protection against vandalism from a single individual. In addition we do not believe that all categories ("High, "Medium" and "Low") need to be subject to NERC compliance.

Question 10

TAPS	See responses to Questions 1, 2 and 5.
GWA	The diverse environments in which assets that make up and support the BES, and the different impacts of individual assets and systems suggest a library of controls with discretion to select those best suited to the environment and impact of an individual system. This will provide a better overall level of security than the "two-bucket" (critical or not critical) approach embodied in CIP 002 V2, by ensuring a comprehensive review of assets, impacts, and allocating security resources to address relative impacts.
MISO	It is not clear what problem the CIP drafting team is trying to solve. Is the CIP drafting team trying to prevent cascading outages and blackouts caused by cyber attacks or are they trying to prevent the BES from ever experiencing any level of impact from a cyber attack. It appears the drafting team is attempting to develop standards based on the latter approach when it would be more appropriate to develop standards designed to prevent cascading outages and blackouts. The standards should not be focusing on a small scale cyber attack on cyber systems that might prevent operational challenges but would not cause a blackout.
SCEG	We agree with this approach. A smart instrument in a remote area requires a very minimum set of controls for Cyber Security, where as a Router connecting a DCS/SCADA to a Control Center would require a much more protective posture
RFC-CIP	Cyber Systems at transmission substations generally operate on specialized programming and processing hardware, have not been developed to accommodate additional security applications, and utilize communications requiring a modem interface. Therefore, security measures would be practically limited to the electronic perimeter, or modem, boundary. However, Cyber Systems at Control Centers are based on a distributed system of client/server hardware and software that communicate over a much wider network system and require careful security posture monitoring at every node.
GEEI	This is an admirable goal, but as a systems manufacturer, it still leaves a great deal of potential variability, when considered on an implementation-by-implementation basis, in the security requirements for any cyber system.
LES	Lincoln Electric System is in agreement with comments submitted by the TAPS organization.
MRO	The MRO NSRS agrees that there needs to be protection but not enough information is provided to apply security controls.

Question 10

MEC	MidAmerican agrees with different levels of protection. However, the levels of protection should be determined based on risk characteristics for the type of cyber asset. As stated earlier, risk includes consideration of probability of an event. For example, assets that are not vulnerable to viruses have no need for antivirus solutions, but the current standards do not provide that flexibility. The protections defined in CIP-005 and CIP-007 should be revised to acknowledge the differences in risk characteristics between relays, controllers, servers, firewalls, etc. This will also significantly reduce the number of technical feasibility exceptions without creating risks to the BES. MidAmerican does not support differentiating based on impact alone. This would add further complexity and not reflect the true risk to the BES.
PSEG	PSEG appreciates that the drafting team recognizes a key objective of the next version of CIP 002 is to develop controls "in such a way as to mitigate risk while maximizing the value of the associated cyber security investment for the industry." PSEG strongly supports hardening of cyber control systems, and applying appropriate security controls. PSEG does not support allocating resources to file and maintain Technical Feasibility Exceptions for systems that are simply not capable of running specific controls. PSEG recommends that the drafting team consider the applicability of each control to various types of devices, rather than forcing a "one size fits all" control than may actually fit none.
MMPA	Different level of protection is a more reasonable approach then the current system where assets either are CCA's or are not. Not all CCA's require the same level of protection and some require TFE's that may fall into a lower level of a multi-tiered approach where a TFE would not be required. Conversely, a non-CCA may require more stringent protection than standard business practices.
SCE	N/A – see comment to question 1.
APPA	If a useful library of security controls can be developed and be appropriately targeted to different types of BES systems and to differentiate between systems based on their importance (e.g., high thresholds for RCs and large multi-state BA/TOP control centers, with low thresholds for small BAs and TOPs, etc.), then the concept paper will be a major advance. However, appropriate balance must be struck between standardization and registered entity discretion.
PAC	PacifiCorp agrees with applying different levels of protection based upon characteristics and categories of specific BES cyber assets. The levels of protection should be commensurate with the risk characteristics for the type of cyber asset.
USBR	Impacts on the BES as the result of Critical BES Assets monitored by or controlled by Cyber Assets is not acceptable irrespective the relative probability of the impact however developed. The existing requirements describe specific criteria and processes which my company must either develop or have documented and implemented to be compliant with the standards.

Question 10

	There has been no demonstrated reason that these requirements are inadequate. The definition proposed by the team in this question (BES Cyber systems are transmission substations, generating plants or control centers) is not realistic or consistent with other reliability standards.
PGE	PGE is not certain how NERC and the Regional Entities will be able to apply their enforcement processes to a flexible system of controls. While a level of flexibility may be appropriate for each entity's implementation, this needs to be weighed against the enforceability of the controls.
FPL	This is a good approach and is similar to what most companies do today. The level of protection i.e. card access, passwords, etc are proportional to the impact that the system could have. One item one clarification should be made regarding external connections as part of a company's Target of Protection. For instance, does this mean a company that relies on data from a foreign company to maintain situational awareness must develop an alternate source of data or require the foreign company to meet the standards.
TECO	We agree with this and strongly encourage the SDT to engage security vendors and SCADA/DCS vendors in the development of this library of controls to ensure that the required controls can be implemented on equipment in the field today as well as equipment developed in the future.

Question 11

11. Section K, Applying Security Controls to the Target of Protection, of the paper introduces the concept of a library of security controls. What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems? What specific challenges would you anticipate in implementing controls from among a library of security controls?

Name	Comment
CLPUD	No opinion. But since this form has no room for general comments, Central Lincoln would like to comment on the applicability of CIP-002. Per the functional model, load serving entities do not own physical assets, and so do not own the BES subsystems and BES cyber systems described. LSEs should be removed from the applicability section.
TNSK	The library of Controls should be based in the implementation best practices of the existing standards.
XCEL	Recommended sources: NIST framework documents (specifically 800-53 and 800-82), ISA-99 The main challenge is translating the security controls designated for information systems and the general information security components of confidentiality, integrity, and availability for the control system environment (where availability has been traditionally stressed as primary, but the other components still need to be addressed).
DOM	It is anticipated there are very few standards that are written to cover real-time data acquisition and control systems using the wide variety of software, hardware, ages, and configurations found throughout the industry. If the Target of Protection was defined more specifically to be aimed at standard cyber devices as mentioned above (firewalls, routers, switches, etc.) it would seem that the library could be based at least partially on standard Information Technology ("IT") protection standards already in place. In fact, standard IT procedures such as user logins, password protection, patch management and malware prevention were examined in the requirements and implementation of Version 1 CIP standards. These are areas of cyber protection that are already well understood and were verified in the current implementation of CIP. This should be used as the basis for any future changes including the development of a library of security controls.
SWPA	We recommend researching all current industry standards and creating a "library of controls" based on those that are most applicable to the systems used to support the BES. We do not agree with adopting another organization's standards verbatim, if they were developed for systems outside of those commonly applied to the BES, without close scrutiny from registered entities. We are also concerned about standards that are also developing and we may or may not have input into their change

	process.
GTC	Vendors should be consulted as a source in developing the library of security controls.
DYONYX	As we read this section, "the drafting team will consider approaches to provide flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities…along with different levels of protection, etc.", in our opinion this whole level of detail is **unsustainable**.
BPA	The utility needs to be able to tailor fit their own library of controls. A predefined library of controls will never be all encompassing – it needs to have options and be flexible. If the library of controls includes a limited list of choices and none actually work for the utility, then the work falls on the utility to try to make something fit where it naturally doesn't fit. Clarification comments. Page 30, lines 15-30, what does "develop a library of controls (requirements) appropriate to the degree and type of protection needed" mean here? Page 30, lines 25-30, specifically note that "operating environments" will be taken into consideration when entities evaluate their approach to protection Page 31, lines 15-20, "all cyber systems related to reliability or operability of the BES are required to implement a security posture commensurate to the level of criticality of the BES Subsystems they are supporting" does this mean if a system supports a critical asset it needs to be covered the with the same controls?
SDGE	As mentioned above, we feel that the library of security controls is key to Section K. They need to be vetted by power system industry experts for practicality, reasonableness, and effectiveness. A library of security controls for a financial institution would be much different that what would be applicable to the power industry. Especially in our field locations, we deal with many inhospitable environments and special challenges related to distance, temperature, etc. If possible, we'd like to have some choices available when implementing an appropriate security control. Please don't lock us in to a small number of controls that may be difficult to implement in our power system environments.
GSOC	The drafting team should consider the following industry standards that exist such as: the NIST framework, ISO/IEC 27002, etc. Another thing that the drafting team should consider is getting input from the vendors of the various cyber systems that they supply, EMS/SCADA, RTUs, Electronic Relays, etc. The vendors should be involved up front to help define the types of

	security controls that should be implemented. If the vendors are not involved up front to help establish security controls that support their products, then it could be difficult and costly for entities to implement the security controls. This could result in the entity having to implement costly workarounds or having to take exception to the standards as stated in Section K.
CUSMO	We recommend researching all current industry standards and creating a "library of controls" based on those that are most applicable to the systems used to support the BES. We do not agree with adopting another organization's standards verbatim, if they were developed for systems outside of those commonly applied to the BES, without close scrutiny from registered entities. We are also concerned about standards that are also developing and we may or may not have input into their change process.
MH	The library of security controls must include provision for layers of protection both inside and outside the ESP and PSP. Protection afforded by isolation, use of private communications and private facilities must be included in this library of security controls. If the library does not accommodate these security provisions then inappropriate security controls may be required. The design of the security controls must provide for flexibility and broad application, so that technically creative solutions, which meet the intent of the standard requirements, are still permitted and they are not excluded by narrow interpretations of the standard requirements. A draft list of security controls should be made available at the same time or before the industry considers any revised CIP-002 standard. Without any information on the security controls the industry will not be able to understand the overall approach and impact to their entity.
NST	We consider the newest revision (Rev 3) of NIST Special Publication 800-53 to be an excellent resource for the development of such a library of security controls. In particular, we note that Appendix D of that document ("Security Control Baselines – Summary") provides a set of recommended controls for High, Moderate, and Low impact information systems that might be useful as a starting point for the creation of comparable baseline profiles for High, Medium, and Low impact BES Cyber Systems. Challenges we see include: • Developing a set of baseline control profiles for BES Cyber Systems that are properly tailored to BES operational environments, address the right sets of identified cyber threats and vulnerabilities (we recognize that reaching consensus on what is "right" may require no small effort), are achievable, and leverage industry investment in compliance with the existing, "-1" set of CIP Standards. • Maintaining and updating a controls library to reflect both emerging technologies and new and evolving threats. • Striking a reasonable balance between allowing for flexibility in selecting and applying controls and requiring, for the sake

	of consistency and overall BES protection, that all BES entities comply with some minimum set of requirements for High, Medium, and Low impact cyber systems. A revised set of CIP Standards based on a "catalog of controls" could, depending on the amount of customization permitted, greatly complicate the tasks of verifying and enforcing compliance.
NPCC	We agree with the concept of a library of minimum requirements, but do not support the concept of a library of controls since requirements are implemented by controls. We suggest one library of requirements for control centers, another for substations and a third for generation. We are concerned about how much time and effort will be needed to create those libraries. We are concerned that existing sources will need so much modification to work with the BES that it is probably more efficient to use industry expertise.
RFC	NIST SP800-53 Appendix F "Security Control Catalog", CoBiT, FISCAM. There is probably an ISO standard as well. The challenges will revolve around achieving a balance of good control with ease of implementation. It is easy to go too far when implementing controls and require more than is necessary to achieve the ultimate purpose
IRC	No comments—We would like to see more details of proposed controls and would support controls similar to how they are currently structured in NIST SP 800-53 Rev 3 and similar ISA publications. The Concept presented in the paper appears sound with respect that those assets listed as HIGH should receive the most stringent controls. NERC/FERC audits should focus on the HIGHS and MEDIUM controls and use self reporting (and spot checks) to address compliance with systems rated as LOW. The level of documentation required for Compliance should be consistent with the level of Risk—HIGH Risk components should have detailed documentation available for review, while Low risk components should comply with basic requirements but not be subject to the same level of documentation required for HIGH systems. Let's not further expand the documentation requirements beyond that currently specified.
AEP	NERC reliability standards focus on the outcomes rather than solutions to achieve those outcomes. Having a menu of controls could inadvertently shift the focus from what to secure and protect to how it should be done which can reduce efficiency and innovation.
WE	Wisconsin Electric recommends starting with current standards (NIST 800-53, ISO 17799) and research current vendor equipment capabilities for relays and control systems around cyber security and internetworking requirements. ANSI standards for specific control systems and relays would be another point of research. The library should be based on what can be accomplished today with a future state direction. Some of these systems have long service lives, so the library of acceptable protective measures will need to allow for older technology that cannot be protected in a certain way without creating a TFE.

Question 11

DUKE	NIST Special Publications SP800-53, 800-32. It may be difficult to determine how to adapt business controls to process computing systems. Another challenge is that technology is constantly changing.
SOCO	As noted in our response to Question 4, cyber security problems do not lend themselves to one-size-fits-all solutions. For example, flexibility is needed to avoid unnecessary duplication which may result based on previously implemented or alternate security protections, or higher level controls.
E-ON	The drafting team should not be developing security controls. The drafting team should be developing standard requirements. Pursuant to FPA Section 215, cyber security standards exist to insure BES reliability by visiting sizable penalties upon relevant entities who fail to secure facilities essential to BES reliability in a manner that complies with the applicable minimal standards. This requires the drafting team to develop requirements that are clear and concise so registered entities readily understand the steps they need to take, or refrain from taking, in order to avoid penalty. The major challenge in implementing controls from a library arises when the methodology currently employed, although perhaps fully adequate in protecting BES reliability, is not part of that library. That is why the drafting team should focus on clear and concise performance requirements rather than prescribing the use of one or more pre-approved security control methodologies
ATC	We are not aware of any source documents but believe that the SDT needs to work with various technical teams that can catalog existing utility practices. ATC does not believe that there is a one size fits all approach that can encompass all entities. The SDT needs to justify the amount of work needed to develop a library of security controls over addressing actual FERC directives.
GWA	NIST Special Publication 800 series, ISA security standards, SANS, and IEEE are all resources. The challenge with implementing security controls from a variety of sources is that the overall approach to each set of controls is somewhat different. The important goal, however, is to provide each asset owner discretion to select a set of controls that provide effective security that are cost-effective, are easily administered and maintained, and are appropriate to the type of asset and its associated reliability impacts. This will ultimately lead to an improved security posture for the BES.
SCEG	The Nuclear Industry has put forth tremendous effort to develop a minimum set of Security Controls to Achieve High Assurance of Adequate Protection. [RG 5.71 (Draft) and NEI 08-09 Rev 2] The list was developed using NIST. Many Controls were modified to take advantage of the Utilities Physical Protection Posture. With different levels of expertise at the various Utilities a Control could have different meanings. Training on the Controls that

Question 11

	are selected as a baseline for High, Medium, and Low Levels of protection would be beneficial to the Industry.
RFC-CIP	The "Library of Security Controls" could be patterned after NIST 800-53 Appendix F " Security Control Catalog" which maps levels of control to the levels of impact of the system being protected. Consider the comment to item 10 above that many security controls would not be able to be applied to a High impact asset. The Library approach could therefore generate an excessive amount of technical feasibility exceptions if such a provision was incorporated into the standard.
GEEI	One of the challenges when selecting from a "library" is that there is always variability in an implementation. Being forced to choose from a particular set of solutions may under-engineer or over-engineer the solution giving no cost or additional risk mitigation benefit. There is no generally accepted / authoritative library of "security controls".
LES	IEEE, EPRI, or ISA. The main challenge would be implementing controls on systems that are not designed for the application, or require utilities to establish a remote connection to update the security control applications on an otherwise isolated networked.
MRO	Inadequate information has been provided in regards to the library of security controls. The library of security controls needs to be developed before a recommendation can be formed. The library of controls might be appropriate in a case-by-case application but a global application should not be made mandatory since every company has unique methodologies.
MEC	MidAmerican would support a library identifying security controls by type of asset. As noted in MidAmerican's response to question 10, standards CIP-005 and CIP-007 need to be revised from a one-size fits all approach. The drafting team should first revise existing controls in the standards by matching controls to the various Cyber Asset types. This foundation is necessary before a gap analysis against other sources can be effective in producing a list of controls by asset types. Risk is the combination of the probability of an event and its consequence. For a control to lower or eliminate risk, it needs to have an impact on lowering probability of an event or lessening the consequence of the event. Only controls that materially lower probability and/or consequence of a significant event for a specific Cyber Asset type should be on the library list for that asset type. Controls that do not materially lessen probability or consequence of a significant event jeopardize the drafting team's crucial undertaking of mitigating risk while maximizing the value of the associated cyber security investment for the industry.

Question 11

	The recommended approach leverages existing progress made under standards 003-009 without completely rewriting or abandoning them and can deliver effective results quicker. To the extent that the security controls in the library are supported in other information technology industry standards, vendors would have greater encouragement to provide information technology that delivers the security controls.
SCE	N/A – see comment to question 1.
APPA	No comments.
PAC	NIST Publication 80-53 - Recommended Security Controls for Federal Information Systems and Organizations. PacifiCorp would support a library identifying security controls by type of cyber asset. As we have experienced in the current standards not all controls can be applied to every type of cyber asset utilized in the industry thus the reason for the introduction of Technical Feasibility Exceptions (TFEs). A library of security controls by cyber asset type would eliminate most TFEs and the administrative overhead associated with these exceptions. If the controls were specific to a category of cyber assets it would likely lessen the challenges of the industry in trying to apply controls to devices that cannot conform to the controls.
USBR	Vulnerability is determined by analysis and test not assumption. The greatest challenge for the team would be to find method that clearly demonstrates the security control solves a real vulnerability.
BRAZOS	ISA-99.
FPL	Although we agree that a library of security controls is helpful, we want to note that it is used as a guideline not as requirements as stated in lines 19-20 of Section K. If the security controls provided are required, it may reduce the flexibility to have vendor solutions implemented in a timely manner.
TECO	We agree with this and strongly encourage the SDT to engage security vendors and SCADA/DCS vendors in the development of this library of controls to ensure that the required controls can be implemented on equipment in the field today as well as equipment developed in the future. NIST and other standards issuing organizations should be consulted. To ensure success, the engagement of security and systems vendors is crucial. We want to also ensure that the controls are cost effective to minimize impact to rate payers who will ultimately be responsible for paying for these controls.

General and Editorial Comments:

Name	Page	Line	Section	Comment	Suggestion
AMER EN-1				This concept paper represents a fundamental shift from any concept that has been used to define critical assets. The concepts outlined in the paper seemingly remove the idea of Critical Assets in favor of a more broad approach. The driving force with reasons behind this concept paper should be stated.	
AMER EN-2				Categorizing cyber systems as described in this concept paper will encompass significantly more cyber assets with no consideration of cost, complexity, or resources needed to protect and remain compliant. There is no supporting information in the concept paper that gives any direction as to the scope of what protective and compliance documentation will be required to remain compliant. Without these boundary guidelines, it is hard to ascertain the value of these concepts as it relates to overall security and compliance burden and its relative value to the protection of the Bulk Electric System.	
AMER EN-3				A great improvement to the risk based methodology if you are going to be forced to apply cyber controls to several new devices is the use of different cyber security protections based on risk and type of cyber asset which is outlined in this concept paper.	
AMER				Many of the NIST controls make no sense for	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
EN-4				control systems. They are written for Ethernet based networks. NIST controls require people intimately familiar with control systems, their configuration, and how they can be protected to develop a set of controls that can actually be implemented. The current criterion of the device needing to have a routable protocol is logical and valuable in determining what you need to protect. Introduction of a concept that envelopes all BES subsystems does little to protect over cyber security for systems that have an "air gap" or use non routable protocols. Including non-routable systems will only increase the compliance burden and provide little to no additional protection to the Bulk Electric System.	
AMER EN-5				Compressive inventory and categorization of BES Subsystems is a large and complex task that would be a significant undertaking if such a study were required annually. It is the intention of NERC and the drafting team to require annual inventory and classification of all assets that comprise the Bulk Electric System? Current CIP standards require 30 days to update any changes in network configuration. Are systems that are part of the BES subsystems that are not inside an electronic security perimeter going to be included in this 30 day window?	
AMER EN-6				The questions outlined can not be answered without an understanding as to what the security controls are going to be based on the categorization of the BES subsystems. This	

Name	Page	Line	Section	Comment	Suggestion
				concept could be beneficial if controls for low risk systems do not overwhelm the benefits of such systems being included within the scope of these regulations. Without such additional information, it is difficult to come to a consensus to answer the included questions in this survey.	
ATC-1a				General Comments: ATC appreciates the amount of work the Standards Drafting Team has already spent on the CIP standards and understands the number of challenges that still must be tackled, but we believe that the proposed *"Categorizing Cyber Systems an Approach Based on BES Reliability Functions"* concept paper does not represent the correct path to improvements. We do believe that the paper contains some good ideas but without fundamental changes the result of this effort may result in a drastic increase in cost and compliance with little or no benefit to the reliability of the Bulk Electric System.	Categorization is not bad but entities must be able to determine the likelihood and severity of an event when categorizing their BES Functions
ATC-1b				It is our understanding that the approach, presented in the concept paper, will result in the elimination of the identification of Critical Assets and the protection of its Critical Cyber Asset (Risk-based Assessment) and replaced with a system were all Cyber Systems will have to be categorized into "buckets" (High, Medium and Low) and then exposed to some level of compliance obligations. The "bucket" concept is critical because it dictates the level of cyber and physical security that entities will have to	Any additional compliance obligations should be limited to only those that have both "High" Asset Impact and Cyber Impact

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				demonstrate compliance with and does not allow for any cyber system to be excluded from compliance. ATC believes that improvements to formalize the process for the identification of a facility's importance (use a Risk-based Assessment approach) is a step in the right direction, but that Reliability Standards should only focus on "High" (Critical/Essential) facilities.	
ATC-1c				ATC also feels that this concept paper fails to address some key questions:	We believe that the concept paper should address these key questions.
ATC-1d				How will this improve reliability? We acknowledge that this will greatly expand compliance obligations but this paper does not address how that alone will improve reliability.	
ATC-1e				What other alternatives were considered? The SDT should provide alternative approaches for the industry to discuss and consider. The SDT needs to provide additional justification for the selection of its proposal and why the alternatives were rejected. (The industry should be allowed to weigh in on the alternative approaches.)	
ATC-1f				What is the SDT attempting to protect against and from what type of event? The proposal seems to indicate that NERC wants to protect everything from everything even if its impact on BES reliability is "Medium", "Low" or	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				none.	
ATC-1g				Why is the SDT abandoning the "probabilistic" approach currently allowed in CIP-002 with a "deterministic" approach? How did the SDT conclude that low probabilistic events were going to be treated the same as high probabilistic events?	This is not done in the planning criteria for example. A lower probability event is not held to the same requirements as a high probability event. Clear criteria should be applied just like for planning criteria.
ATC-1h				What is the cost impact of this proposal? This should be looked at from the perspective of a small, medium and large entity. Based on our understanding it would seem that a small entity that does not have any Critical Assets will likely incur a large increase of cost. In contrast an entity that has Critical Assets may not see an increase in compliance for those elements but will see an increase in cost associated with "Medium" and "Low" facilities. Because of the possibility of increased cost, we believe that the SDT needs to perform a Beta Test.	
ATC-1i				Beta Test: (This was suggested as a possibility on the Webinar conducted on August 25th) ATC believes that the SDT should perform a beta test to help the SDT understand the impact and potential cost associated with this proposal. In addition, a beta test would help the SDT work through the undeveloped elements of the concept and learn about any significant weaknesses or flaws with the concepts before including them in	ATC believes that the SDT needs to perform a Beta test and publish the results. The publish document should address our concerns at a minimum.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				mandatory Reliability Standards. This will also aid the industry to understand the potential impact in moving to this type of Reliability Standard.	
ATC-1j				The beta test should reveal the following: Comparison of existing Critical Cyber Assets to Cyber System that are classified as "High", "Medium" and "Low".	
ATC-1k				Does the number of Critical Cyber Assets equal the number of "High" Cyber Systems? If so, are they the same assets? If not, what is the difference?	
ATC-1l				What would be the cost to protect the additional "High" Cyber Systems using existing CIP standards?	
ATC-1m				What is the potential cost to protect "Medium" and "Low" cyber systems? (NOTE: It's our understanding that the SDT has not started to document what are the compliance obligations for "Medium" and "Low" cyber systems which may make determining cost difficult but the SDT should make a good faith effort to understand those cost.)	
ATC-1n				Partial Picture: The concept paper provides only a partial picture of the impact associated with this type of	The concept paper needs to provide more of the picture in order for the industry to understand the totality of moving this effort forward.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				fundamental change to the CIP standards because it does not get into the compliance elements (Cyber and Physical security) associated with the three "buckets". We believe that the SDT must provide a more complete picture of the changes before moving ahead with this concept paper. When the paper refers to the loss of a BES subsystem or subsystem element, it should be more clear that this only applies to loss of the subsystem or element due to a cyber system attack (e.g. take control over, block control of, falsify monitoring, block monitoring, change settings, etc.)	
ATC-1o				FERC Direct Changes: Given that FERC did not direct these changes, it would be very helpful for the SDT to identify why they feel it is necessary. (What problems or issues are being addressed because of this new approach? and, who believes them to be problems or issues?) ATC believes that the proposed concept paper is not needed to address the remaining FERC directives contain within Order 706, and that it would be best for the SDT to address the remaining FERC directives contained within Order 706.	The Concept Paper needs to better identify the purpose of this change along with why the industry should be supportive of this new proposal. ATC believes that the SDT should focus its attention on actual FERC directed changes and then consider if it is prudent to make this paradigm shift.
BGE-1				In definitions - need to add BES Reliability Functions	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
PSEG-2				The paper mentions "Critical Cyber Assets" in very few places, instead focusing on the phrase "BES Cyber Systems". Under the new concept, will all systems under the Target of Protection be seen as equivalent to Critical Cyber Assets in Versions 1 and 2, or are only those systems classified as BES Cyber Systems equivalent to Critical Cyber Assets?	
SOCO-1				In general, there is a concern that if we modify the standard to encompass so many more components, systems and subsystems, how will anyone be able to make this standard compatible with the interoperability standards/technology?	
SOCO-2				If this paper is used to revise CIP-002 will other CIP Standards be revised at the same time? It appears that the changes described in this paper would be difficult to use if Standards CIP-002 through CIP-009 are not revised to complement each other. As a result, the revised CIP-002 should become effective along with the other applicable revised CIP Standards, guidelines and implementation plans.	
SOCO-3				To be consistent with NERC's authority under the Federal Power Act, references to "reliability or operability" should be replaced with "reliable operability."	
TECO-				TEC would like to recognize the effort and	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
1a				creative thinking of the Standards Drafting Team in creating the concept paper for categorizing cyber systems. We agree with and support the comments of the Edison Electric Institute related to this draft. In addition we would like to stress the following points.	
TECO-1b				1. The Concept paper introduces potentially significant change to the current methodology to determine cyber systems to be protected. This has the potential to increase the scope of work as standards CIP-003 – 009 are applied to the new set of cyber assets. It will significantly increase the effort required by the industry in terms of resources and costs. While we support the concept of the new methodology, we strongly urge NERC and the SDT to allow for and build in adequate time for the industry to come into compliance when drafting the actual revision to CIP-002.	
TECO-1c				2. In order to address the Technical Feasibility Exception issues, we believe the SDT will need to modify or allow for more use of or methods for providing mitigating controls to provide regulatory compliance.	
TECO-1d				3. We strongly support the SDT concept of ensuring that the security controls and	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				requirements be commensurate with the BES reliability impact of a particular cyber system.	
TECO-1e				4. It is unclear from the concept paper where the SDT is going with the routable protocol. We believe the SDT should use caution in evaluating expansion of the scope beyond that due to the vast amount of equipment in the field which does not have the ability to comply with the technical controls of CIP-003 – 009.	
TECO-1f				5. We strongly encourage the SDT to engage the security and SCADA/DCS systems vendors in the process of developing controls for these systems.	
TECO-2				Are Cyber Systems equivalent to Cyber Assets? That may need to be explained/defined in the document as the industry has been considering cyber assets.	It would at first appear that Cyber Systems relate to software/hardware that work together to provide certain functionality. However, in your examples, you list things such as relays, front end processors, etc. What is the difference between cyber systems and cyber assets. Can systems be discrete pieces of hardware?
SOCO-4	General	-	-	The term BPS is used in the "Defining Critical Assets" & "Defining Critical Cyber Assets" standards rather than BES.	Use a common term for the "system" throughout the standards.
SOCO-	3	14		Editorial	Replace "*Based on BES Reliability*" with "Based on impact

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
5					on BES Reliability".
AWEA-1	3	15	Executive Summary	It is concerning that the approach to cyber security standards outlined in this paper seems to supersede existing NERC efforts to develop cyber security standards. In particular, the processes that have already been developed for identifying and protecting critical cyber assets based on risk-based analysis seem like a valuable basis from which to work in developing future processes. A large amount of effort has already been devoted to developing these processes, which seem to be very effective and enjoy stakeholder support, and this paper does not offer any reason why these processes are inadequate and need to be superseded. The abrupt transition from existing cyber security efforts to the approach offered in this paper also exposes the industry to significant uncertainty about what form cyber security standards will ultimately take, reducing industry's ability to comply with these standards in an efficient way.	Risk-based processes that have already been developed for identifying and protecting critical cyber assets should form the basis of any newly proposed approaches.
ATC-2	3	35	Executive Summary	ATC does not believe that the concept paper identifies the FERC directive that this paper hopes to address.	The paper needs to clearly identify the FERC directive that is being addressed. In addition, the paper needs to identify the alternative approaches that were considered along with why the SDT reject the alternate approach.
SOCO-6	3	41		Editorial	"drafting team" should be replaced with "Standards Drafting Team (SDT)".

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
SOCO-7	3	50		Editorial	Define first occurrence of SDT.
ATC-3	4	20	Introduction	The following sentence is not clear: "FERC's comments in its Order 706 approving the Cyber Security Standards as well as common perceptions…"	What are the common perceptions being considered and who do they represent? The purpose of this effort should be to address FERC directives.
DYONYX-1	4	27	B	We believe the ALR definition is too broad for use in categorizing systems that impact the reliability or operability of the BES. For example, just because a BES infrastructure is not designed with sufficient capacity to supply "the energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of the system components" does not mean certain elements of the infrastructure need to fall under the CIP Reliability Standard. The issue is with the design, not the additional protection required.	Develop a more definitive set of reliability criteria for use in determining Critical Assets / BES Sub-Systems. Eliminate ALR # 6.
ATC-4	4	30	Introduction	ALR definition is too vague to be an acceptable basis for the CIP standards. For example: Item 2 – the definition/criteria for "performs acceptably" are open to wide interpretation and may vary for different conditions [Is the loss of less than 1,000 MW of load acceptable for cyber system contingencies?]; the definition/criteria of "credible Contingencies" are open to wide interpretation (including probabilistic considerations) [What level of cyber security allows the associated cyber	This effort should focus solely on those things that are essential/critical to the BES.

Name	Page	Line	Section	Comment	Suggestion
				system contingencies to be deemed not credible?]; Item 5 – the timeframe/criteria for "restored promptly" are open to wide interpretation, is restoration within a week acceptable for cyber system contingencies; Item 6 – the "ability to supply . . . power and energy . . . at all times" for any contingency is impossible whether it is a cyber contingency or something else; besides adequate has the meaning of the supply continuity being good enough, not perfectly.	
ATC-5	4	30	Introduction	A key premise of the paper is that proper cyber system security categorization is based on the identification of Reliability Functions that are essential to achieving an Adequate Level of Reliability (ALR). However, compliance with the NERC Transmission Planning Standards of TPL-001-0, TPL-002-0, and TPL-003-0 assures an adequate level of reliability is achieved for BES subsystems based on meeting acceptable system performance levels for different categories of contingency events for an appropriate range of system conditions. Bulk Electric Systems that are built and planned to meet these Transmission Planning Standards should not have any BES subsystems that are essential to achieving the adequate level of reliability characteristics. On the other hand, cyber attacks are expected to produce events that fall into the TPL-004-0 (Extreme Event) category of contingencies, which are not subject to any set of adequate reliability limits. If a set of acceptable system performance limits/characteristics would be developed for	This effort should focus solely on those things that are essential/critical to the BES.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				cyber attack contingencies, which are extraordinary, then it would be reasonable to expect these limits/characteristics would different from (beyond) the adequate level of reliability limits/characteristics.	
MGE-1	4	31-44	B	This section states that the NERC Adequate Level of Reliability (ALR) will be used as a test to see if a cyber system is required to maintain a reliable BES thus, to ensure ALR. Entities are to use ALR as a measure while formulating their BES Subsystem components to see the BES Reliability impact. All NERC Standards have this as an imbedded intent, which produces a reliable BES.	Identification of BES Subsystems is required to avoid instability, uncontrolled separation, or cascading outages. (as stated in section 215 of the Energy Policy Act authorized by Congress).
E-ON-1	4	35	B	The second BES characteristic requires the BES perform acceptably after "credible" contingencies. The term "credible" is too subjective and leaves the identification of BES functions far too open-ended. After the fact, any series of events or combination of events, no matter how improbable, can be said to have been a credible contingency.	Replace the word "credible" with "pre-identified credible."
GEEI-1	4	35	B	"Credible Contingencies" is not clearly defined	Define the term versus leaving REs to interpret.
SOCO-8	4	35		Editorial	Replace "credible Contingencies" with "credible events".
XCEL-1	4	35	B	ALR Characteristic #2 - please clarify what defines a "credible contingency".	Define "credible contingency"

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
E-ON-2	4	42-44	B	The sixth BES characteristic reads: The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components. E ON U.S. believes that this is not a characteristic of BES reliability. BES reliability requires that generation and load be balanced, not that the BES has the ability to supply the energy requirements of electricity consumers at all times. The ability to meet the demand of electricity consumers at all times is a measure of system adequacy and a characteristic of service, not BES, reliability. Section 215 (a)(4) of the Federal Power Act provides that [t]he term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements. Section 215 does not mention maintaining an ability to supply the energy requirements of all electricity customers at all times. Including all cyber systems that support all the functions required to supply electricity to end use customers will greatly, and needlessly, increase the number of cyber assets subject to CIP requirements.	Strike characteristic six from the list. Only the first five characteristics of the BES set forth in NERC's definition of Adequate Level of Reliability are relevant to identifying the BES functions and BES cyber systems/

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				Cyber systems that support an electric utility's ability to supply the aggregate electric power and energy requirements of its electricity consumers at all times should not, for that reason alone, be subject to Version 3 CIP cyber security standards.	
FPL-1	4	46-49	B	These sentences give the impression that the objective/goal is to achieve all of the characteristics of the NERC ALR. It is inconsistent with the heading over the Executive summary section that says "an approach based on impact. The overall approach and process are useful and helpful. These sentences create concern and are a distraction from the balance of the paper which allows categorization based on impact and varying levels of protection.	
FPL-2	5	9		Phrase " if it directly performs one or more of the identified functions" speaks to identified functions which are not previously mentioned	"if it directly performs one or more of the functions contained in Table 1 on page x"
SOCO-9	6	11		Editorial	Replace "credible Contingencies" with "credible events".
GEEI-2	6	30-40	Figure 1	No mention of Distributed Generation	Future widespread implementations of distributed generation capabilities are likely. Include distributed generation as a potential BES subsystem if NERC feels that there is potential for impact to the BES.
GEEI-3	6	30-	Figure 1	No mention of Demand Response or AMI	Recognizing that this is potentially an out-of-scope item, improperly managed and/or secured Demand Response

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
		40			and AMI systems have the potential to have an impact on the BES. Include Demand Response and AMI systems if NERC feels that there is potential for impact to the BES.
ATC-6	7	15	Introduction	ATC does not agree with using impact of an event as the only attribute for determining categorization. We believe that entities should also be allowed to consider the probability of an events occurrence.	The paper must allow for the consideration of or credit for existing cyber and physical security investments.
DUKE-8	7	23		The paper states that nuclear are excluded. Since FERC has ruled that nuclear plants should be considered under CIP, his statement of exclusion is confusing. Are nuclear plants part of the analysis – or not?	
FPL-3	7	31-34		This is redundant and just repeats which was stated above.	Recommend removing.
SOCO-10	7	44		Editorial	Replace" standards drafting team" with "SDT".
ATC-7	8	15	Introduction	Why is the SDT replacing a probability approach to cyber security with a deterministic approach?	The industry deserves a complete explanation as to why the SDT is moving to this approach. (See our earlier comments)
IRC-1	8	15	B	Statement says: "this methodology parallels general approaches to risk management practices." Concur with this approach. The general risk analysis considers not only	Since this concept paper greatly increases the scope of the systems that will be auditable by NERC, suggest that business impact be a factor in the analysis to be a truly holistic risk methodology and approach.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				technical impact but also business impact. We already know that version 2 of the standards will remove business impact factors for risk analysis.	
DYON YX-2	8	17	C	Table 1: Contingency Reserve / Peakers: The "Unit capable of starting in 15 minutes or less" is not appropriate for application to the CIP Reliability Standard. Application of this provision gets into the "reliability" of the "Contingency Reserve" itself, e.g., the "reliability" of the components used to provide "reliability".	Eliminate the "Unit capable of starting in 15 minutes or less provision".
MGE-2	8	25 and 26	B	Do not agree with the below statement; "but should be prepared to have their assumptions challenged, as this represents a paradigm shift for experienced operating personnel". The statement may be proof that no matter how an Entity maps and identifies BES Subsystem, the Entity will be challenged by an auditor on their methodology. This is why the SDT must give the industry clear guidance on BES Subsystem identification.	Remove the statement.
PGE-1	8	26	B.	PGE believes that the Standard Drafting Team's efforts to introduce a "paradigm shift" to the CIP Standards is premature and unwarranted. PGE has invested significant time and resources in complying with Version 1 of the CIP Standards. Shifting to a new paradigm could result in significant changes to PGE's cyber security program, in some areas potentially forcing PGE to greatly extend that program beyond what is	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				necessary to maintain reliability and security. The Standard Drafting Team has not presented sufficient rationale to justify this potentially burdensome and costly paradigm shift.	
ATC-8	8	35	Introduction	The SDT needs to provide a more complete picture of the impact of this change in CIP Standards. What is the compliance obligations associated with "High, "Medium" and "Low". (Cyber and Physical)	More detail is needed
BGE-2	10			Table 1 - Section C - need to be stronger and form the matrix as a requirement not a suggestion	
E-ON-3	10	10-15	Table 1	As E.ON U.S. understands it, any generating unit, or combination of units with common mode of failure, with output in excess of available Contingency Reserves would be identified as a BES subsystem. It is often the case that generating units reside within the boundaries of a contiguous piece of property, often sharing, for example, bus work, other electrical interconnections, or common fuel supply. Table 1 suggests that all facilities within these multi-unit generation campuses would be deemed BES subsystems and thus all associated cyber systems would be required to conform to NERC cyber security requirements. This approach will result in a considerable increase in the number of systems, down to and including protective relays, that must comply with the as yet undefined Version 3 requirements. E.ON U.S. questions	Blackstart generating units only should be deemed BES subsystems.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				how many of these facilities are in fact essential to maintaining BES reliability.	
DYON YX-6	10	17/ 32	C	Transmission "busses" are too low of level of detail for relevant analysis. The entire transmission substation or switchyard is more relevant for analysis.	Eliminate "busses" from the BES Subsystem examples.
DYON YX-3	10	18/ 38	C	It is difficult to understand how a single "protective relay" can be a "cyber system" by itself that impacts the BES. A group of protective relays could certainly impact the BES.	Eliminate "protective relay" as an example of a "cyber system".
AWEA-2	10	18	Contingency/ Peaker Reserves	In the Contingency Reserve/Peakers Category, the criteria of "Unit capable of starting in 15 minutes or less" is identified. Almost any unit, even nuclear units, can "start" in 15 minutes or less. Few can reliably get to some designated load level in 15 minutes or less. That is the real test.	The criteria should be modified to clarify that it specifies that the plant be able to be dispatched a certain load level in a certain amount of time.
XCEL-2	10	18	Table 1	It is unclear the relevancy of the bullet "15 minute or less" in the criteria - what is this?	Clarify what justifies the "15 minutes or less" criteria and how it applies
RFC-1	10	19	C	For the "Contingency Reserve" row, "Criteria" column – It says "Unit capable of starting in 15 minutes or less". Doesn't the unit actually have to ramp up within 15 minutes to the amount of reserve it is supposed to provide?	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
DYON YX-4	10	21	C	We do not agree with inclusion of the following: "Transmission facility or facilities whose loss or compromise may result in the loss of resources identified for Contingency Reserves". Again, the application of this provision gets into the "reliability" of the "Contingency Reserve" itself, e.g., the "reliability" of the components used to provide "reliability".	We cannot agree that transmission facility or facilities whose loss may impact the resources for "Contingency Reserves" are applicable for the CIP Reliability Standard. Theoretically, this could be ALL transmission substations, etc. However, we can envision the identification of a transmission facility or facilities whose loss may result in the loss of the single resources that by itself exceeds the "Contingency Reserve" similar to the loss of transmission facility or facilities that impact the availability of a black start unit.
DYON YX-5	10	25	C	Cyber System Examples: "Plant control room" is not a good example of a cyber system. The definition of "control room", along with "control centers", is a troubling set of terms. It is not the "control center" or "control room" that is a "cyber system", it is the underlying "system" within the control room or control center that is important.	Eliminate "plant control room" term as an example of a cyber system.
DYON YX-7	10	29	C	We question the relevance of analyzing the loss of a single resource (or combined resource sharing a common mode failure) and the impact on under-frequency conditions. It is simply not a condition which occurs. In this scenario, voltage or VAR analysis will supersede any need for under frequency condition analysis.	Eliminate this scenario
AWEA-3	10	30	Load Balancing	In the Load Balancing and Frequency Response/Support Category, the phrase "Single resource or combined resources (sharing a common mode failure) whose loss or compromise may result in under-frequency" is used to identify	The test should be whether the loss results in unacceptably low frequency or rate of change of frequency.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				critical resources. Any unit, even of very small size may result in under-frequency if lost.	
RFC-2	10	30	C	For the "Load Balancing" row, "Cyber" column – Should AGC be listed separately or is it assumed to be part of the EMS?	
XCEL-3	10	30	Table 1	We are concerned b/c frequency response and support are difficult to characterize.	Clarify what the specific criteria for frequency response and support are
WE-1	10	40	C, Table 1	We do not consider a plant control room to be a cyber system.	Remove plant control room from cyber system examples.
RFC-3	11	11	C	For the "Voltage Support" row, "Cyber" column – Should EMS and UVLS be listed?	
DUKE-1	11	25		If Constraint Management is retained as a BES Function that is in the scope of this method, BES Subsystems to support that should include constraint management tools that the industry provides such as the Interchange Distribution Calculator.	
DYON YX-8	12	10	C	Control Center not applicable	Eliminate the use of the term "control center"….source of much confusion whereby the "systems" concept should resolve; see comment for Question # 1.
WE-2	12	10	C, Table 1	Cyber system examples: We use the acronym DCS for generation "distributed control systems".	Consider adding "distributed control systems" for generation assets as a cyber system.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
SOCO-11	12	28		Editorial	Replace "centre" with "center".
RFC-4	12	29	C	For the "Control and Operation" row, "Criteria" column last line – "centre" should be spelled "center".	
E-ON-4	12	30-40	Table 1	Table 1 suggests that the collection of status and alarm points the monitoring of which is essential to BES reliability is both a BES subsystem and cyber system. Such a classification would potentially necessitate applying the full suite of cyber security requirements to, for example, field wiring from RTU to alarm/status contact.	Clarify the intent of this section.
DYON YX-9	12	49	C	The term "element" is not clear	Eliminate the term element; too low of level of detail.
DYON YX-10	12	50	C	We understand that load is important to have in the restoration process but load is typically available from multiple sources and specific loads cannot necessarily be relied on for use in the restoration process.	Eliminate "load distribution feeders" from list of possible BES Subsystems; otherwise, this would imply ALL load feeders should be available.
DUKE-2	12	51		Distribution feeders should not be included – this greatly expands the scope of the standard.	
WE-3	13	20	C Table 1	Protective relays may or may not be "cyber systems". An electro-mechanical relay should not	Modify "protective relay" with "solid state" or "microprocessor based".

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				be considered a cyber system.	
RFC-6	13	24	C	For the "System Stability" row, "Cyber" column – perhaps EMS, SCADA, and RTU should be added.	
RFC-5	13	31	C	For the "System Stability" row, "Criteria" column – "wide-area spread are" should be "widespread area".	
E-ON-5	13	35-45		Water heater and air conditioner loads are sometimes controlled by utilities to lower demand during peak usage periods. Such programs complement and improve the efficiency of utility operations and ought to be encouraged. While conceivable such systems may be essential to BES reliability, in practice these tools are complementary and often far down the list of reliability tools relied upon by operators. Subjecting utilities to the potential penalties that result from violation of NERC standards risks discouraging the implementation of programs that would otherwise provide operator optionality and economic benefits to ratepayers.	Remove apparent presumption that DSM and load management systems are essential to BES reliability.
DYON YX-11	13	40	C	We are concerned about how these terms (load management control systems, Smart Grid, etc.) and offered for consideration.	We agree the design of Smart Grid infrastructures should consider large (> 300MW) single point "control scenarios".
SDGE-	13	45	Table 1	A BES Subsystem example that could be in-	As you know, there are many different types of "Smart Grid" systems, involving different types of equipment and

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
1				scope is shown as "Smart Grid"	functions on both the Transmission and Distribution systems. The term "Smart Grid" really needs to be defined more fully so that the intended audience can understand exactly what functions are being called out as "in-scope".
DUKE-3	13	48		It is not clear what is meant by Dynamic Feeder Management System – does this include distribution assets?	
DYON YX-12	14	10	C	We are concerned about measures to protect available "remote relay setting" provisions from cyber attack. We agree it is important but other than protecting the network with which they are accessible,	
GEEI-4	14	15	C	"Physical Security System" is listed under Cyber System Examples. As worded, it is not clear what the cyber element of the example is.	Change "Physical Security System" to Electronic Access Control Systems, Electronic Asset Access Control Systems, or similar.
RFC-7	14	17	C	For the "Other" row, "Cyber" column – Consider adding, "cyber systems like Distribution Management System (DMS), Windows Active Directory Servers, etc."	
IRC-2	15	28-32	D	Statement indicates that:" Identical cyber systems may also be implemented in different environments, resulting in different impacts on the BES functions they support. …a control system in a small generating facility may have a different reliability impact on the BES than an identical	There needs to be a clear statement related to the security of the interconnectivity between the control systems of all entities with those of the RC/BA/TOPs.

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				control system operating a larger or several generating facilities." Should go further.	
BGE-3	16			Section E - mapping needs to be clarified to tell us the entity-determined criteria for graduating the impact scale will meet all compliance requirements	
DYON YX-13	16	15	E	Again, why have three (3) levels (see comment to question # 1). The NERC Bulk Power System Event Classification Scale in its current form is totally insufficient for this purpose. This is way too much detail.	We recommend caution be applied when using other terms or parameters from other Standards for application to the CIP-002. Something as sensitive as CIP-002, which has significant impact on the application scope of the CIP Reliability Standard, should be quite clear in their use of terms and definitions.
IRC-3	16	`17	E	Not sure why "situational awareness and operational control" are mentioned in the last part of the sentence.	Delete the phrase "such as situational awareness or operational control" from the last sentence.
SOCO-12	16	21		Editorial	Replace" standards drafting team" with "SDT".
GEEI-5	17	15-30	F	The examples lack detail and therefore are still vague.	Provide more detailed examples that REs can apply.
GEEI-6	19	N/A	G	Lack of clarity.	Detailed case studies or examples would be helpful.
DYON YX-14	19	15	G	We believe this type of classification is too detailed and not relevant for use herein. We are also not sure if the fact that a cyber system that	See comments from Question #1

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				impacts multiple non-BES Sub-Systems "together" of which impacts the reliability of the BES is taken into consideration here.	
GEEI-1	19	24-32	G	Confidentiality, Integrity, and Availability carry different meanings in different contexts, even within the same system.	Add definitions to Appendix A that clearly define what NERC believes Confidentiality, Integrity, and Availability to be given the diverse sets of scope that encompass the BES.
GEEI-7	19	24-32	G	Confidentiality, Integrity, and Availability are not independent variables to be measured. One cannot rate a systems Confidentiality without also rating its Integrity, etc.	Make the language clear, or define the terms more clearly. Alternately, remove the terms. The statements hold meaning even after the removal of the three terms and replacement with a more generic "compromise" adjective.
EAGLE -1	19	35	G.	"This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES Subsystems as shown in Figure 3." Question: Does the methodology recognize that a single Cyber System may support a single function for multiple Responsible Entities? As an example, a single control room provides SCADA for 5 separate GOPs. Each Responsible Entity could categorize the single Cyber System differently based upon the affect the loss of availability of its generation to the BES.	
DYON YX-15	21	11	H	This approach is a single system analysis approach which misses the point. We just do not believe this concept is applicable for control systems and issues associated with the reliability of the BES.	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
ATC-9	21		Table 2	The logic of the evaluation matrix is inverted. For example, if the impact of a BES Cyber System on an associated BES Subsystem is "High", but the impact of the associate BES Subsystem on an associate BES Function is "Low", then the Cyber System Category should be "Low" because the resultant impact on the associated BES Function is "Low". An appropriate title and different row and column labeling of the evaluation matrix would help clarify the meaning and usage of the table. A suitable title for the table might be, "BES Function Impact". The better heading for the first row would be, "Subsystem Impact on BES Function". The better heading for the first column would be, "Cyber System Impact on BES Subsystems. For the 3x3 table example in the paper, the revised table would have one "High" cell, three "Medium" cells and five "Low" cells.	
IRC-5	21	Tabl e 2	H	Header should be changed from "Asset" Impact to "System" Impact as the focus of the concept paper is on critical systems and not critical assets.	
WE-4	23	20	I	Interconnected cyber systems are a concern and need to be accounted for when they use routable protocol.	Change "Interconnected Cyber Systems supporting…" to "Interconnected Cyber Systems using routable protocol supporting…"
GEEI-1	23	29-30	I	"Non-repudiation" is part of integrity - it seems redundant to list them both.	Remove non-repudiation, and include non-repudiation in the definition of Integrity in Appendix A.
DUKE-	23	30		This paragraph introduces the concept of non-	

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
4				repudiation requirements in addition to confidentiality, integrity and availability – this seems like a further expansion of scope.	
DUKE-9	23	41		Are the Infrastructure Cyber Systems referenced here the Infrastructure Support Cyber Systems defined on p 32, line 43? If not, a definition is needed.	
NST-1	29	11-33	J ("External Cyber Systems")	We believe that declaring Responsible Entities would own and be responsible for mitigating risks associated with Target of Protection elements they neither own nor control would provide Entities with a powerful incentive to ensure they never include third-party cyber systems and/or interconnections in their defined Targets of Protection.	We believe that solutions to the problem of having to depend on and/or trust input from outside a given company's zone of control will likely require the establishment of bilateral or multilateral service level and information security agreements among Responsible Entities, perhaps under the aegis of NERC and/or Regional Entities. We recognize such efforts could be hampered by existing antitrust regulations and FERC constraints on information sharing, but we are convinced the current proposed approach will not achieve the SDT's goal of protecting third-party cyber systems and interconnections that are important to overall BES reliability and operability.
WE-5	29	20	J	Responsible entity with operational responsibility should identify and manage risk of the BES cyber system- requires additional dialogue.	More clarification of roles and responsibilities for both the BES cyber system owner and operator would be good.
IRC-4	29	25-28	J	Many utilities have third-party vendors providing key control system maintenance and operational support. While the utility may specify what security controls the vendor must provide, it is difficult and almost impossible for the utility to	The new standards should address a new category for key electricity sector vendors and require their compliance with applicable security controls to support reliable operation of the BES. For example, vendor EMS components should be designed and developed to allow

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				enforce those controls on vendors and their staff.	compliance with CIP stds. Additional, the ERO and REs should be able to audit those vendor Operations and Maintenance centers to ensure compliance with applicable sections of the CIP stds.
PSEG-1	29	25	J	The example states (lines 25-30) that Alpha "owns the risk and has the responsibility to mitigate the risk…" Does that give Alpha the right to force Beta to endure a compliance burden, or does the example require Alpha to cover the compliance burden at Beta themselves? If Alpha and Beta do not agree, what sort of process will arbitrate the situation?	
DUKE-5	29	27		It is not clear whether this means Utility Alpha is responsible for protecting the interface with Company Beta from unauthorized access or if it means Utility Alpha is responsible for mitigating the risk of Company Beta's system being compromised.	
BGE-4	30			Section K - need clearer direction in applying the controls	
DUKE-6	32	35 and 40		What differentiates operations support workstations from HMI Workstations?	
XCEL-4	33	6	Definitions	The definition of "Collateral Cyber Systems" needs to be clarified to ensure the scope is not	Revise definition of collateral cyber assets to narrow the scope to those assets specifically connected to BES cyber systems within the same network that will fall under the

General and Editorial Comments

Name	Page	Line	Section	Comment	Suggestion
				wide open.	same target of protection because of connectivity.
DUKE-7	33	11		The use of "evaluates" in this sentence does not make sense, and this seems to be the first place that the concept of resiliency is introduced in this paper. It seems this concept should be explained in section I if it is going to be used here.	

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Categorizing Cyber Systems:

An Approach Based on BES Reliability Functions

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

August 25, 2009

to ensure the reliability of the bulk power system

Presentation Outline

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Background and History
- CIP Version 3 Key Guiding Principles
- Purpose and Approach of Concept Paper
- BES Subsystems and Cyber Systems
- Proposed Categorization Methodology
- Target of Protection
- Conclusion and What's Next

Background

- FERC's Cyber Security Order 706 directed extensive modifications of CIP-002 through CIP-009 (Version 1)
  - Address the near term specific directives ➔Version 2
  - Submitted to FERC for Approval (May 22, 2009)
- Current Phase – Starting to address all remaining issues from FERC Order 706 and as raised by industry in the SAR ➔Version 3

CIP Version 3

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Initial Considerations

- Addressing issues with CIP-002-1 approach and methodology
  - Concept paper ***Categorizing Cyber Systems An Approach Based on BES Reliability Functions***
- Looking at NIST and other frameworks for suggestions and guidance

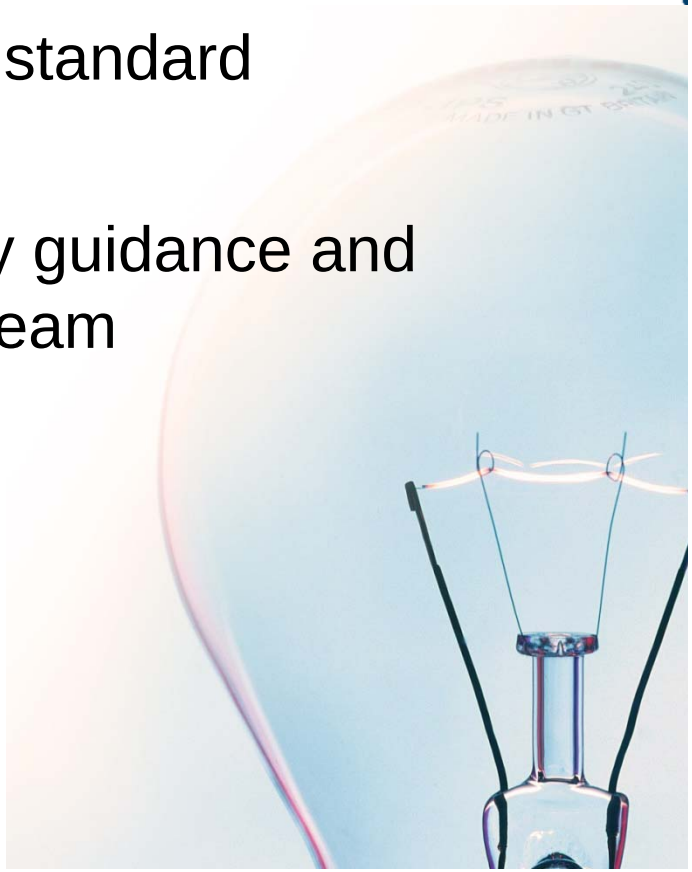
CIP Version 3 Key Guiding Principles

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

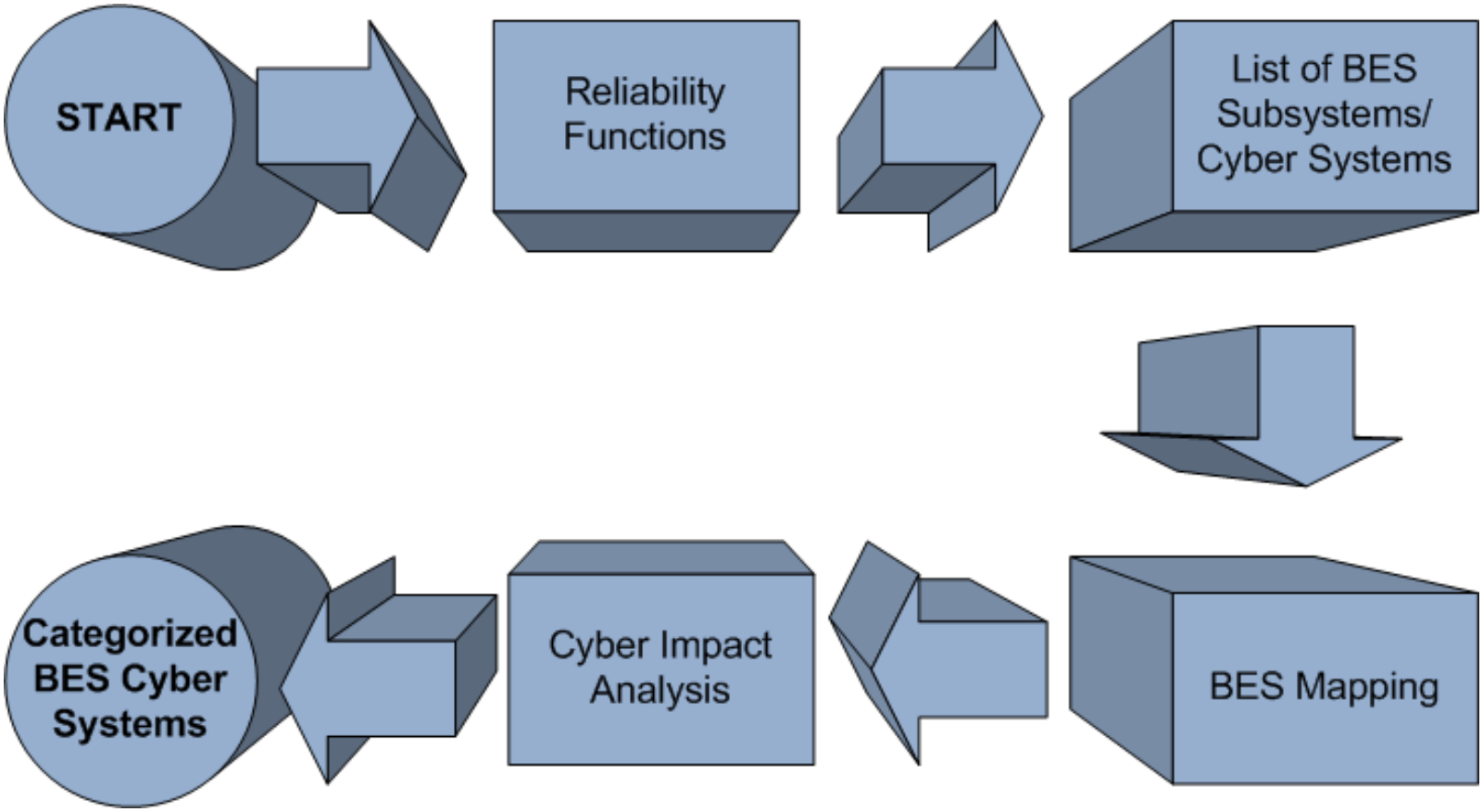
- The CIP Standards will:
  - Build on work already done complying with Version 1, including industry's experience and investment
  - Address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations
  - Provide Entities with reasonable flexibility in applying equivalent security controls on the basis of compensating controls, cyber system characteristics, and operating environment considerations
  - Include all Cyber Systems impacting the reliability of the BES in scope

Concept Paper Purpose

- The purpose of the concept paper is:
  - Address foundational issues at a high level
  - Create an approach for Version 3 standard development
  - Provide an opportunity for industry guidance and direction to the standard drafting team



Concept Paper Approach



Differences Between Versions

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Version 1 / Version 2

- Asset types to consider
- Critical Assets
- Critical Cyber Assets
- Critical / Not Critical
- “One size fits all” security

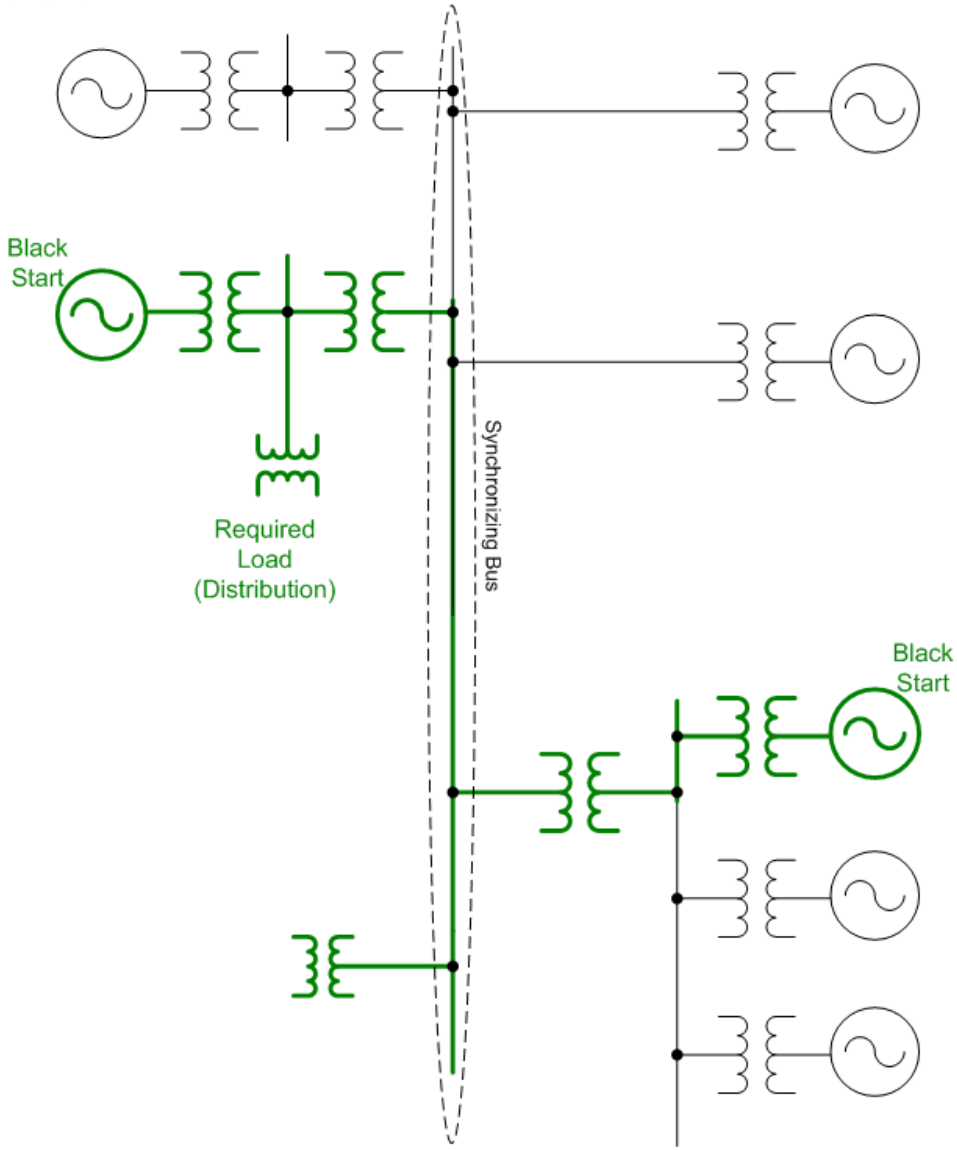
Version 3

- Reliability Functions
- BES Subsystems
- BES Cyber Systems
- Impact Levels
- Security commensurate with BES reliability impact

BES Subsystem

- BES Subsystem: The set of BES assets necessary to perform or support function(s) necessary to maintain an Adequate Level of Reliability (ALR)
  - May be defined as a piece of equipment, facility or system
- Cyber Systems performing or supporting functions necessary to maintain an ALR will be considered as both a BES Subsystem and a Cyber System
  - Captures both the reliability impact and the cyber impact
- BES Subsystem Examples
  - Restoration System (Black Start generators, cranking path elements – transformers, lines, reactive devices, load)
  - Load Control System (centralized, automated, programmable)

BES Subsystem Example - Restoration



BES Subsystem for Restoration

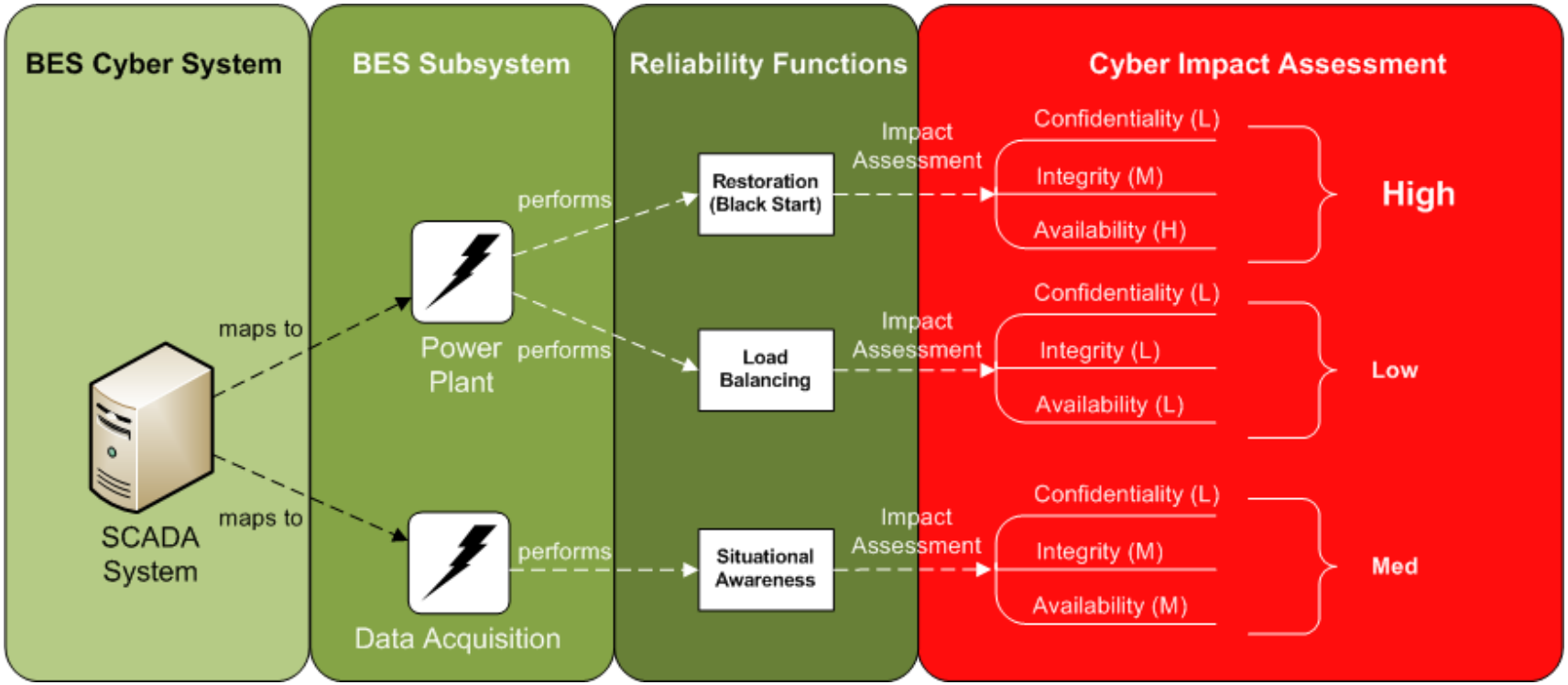
Cyber System

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Entities define their Cyber Systems to maximize efficiency in secure operations
- Cyber System Examples
  - EMS/SCADA System
  - Generation Control System (at the Plant)
  - Substation RTU/PLC
  - Microprocessor–based Relay

cyber security

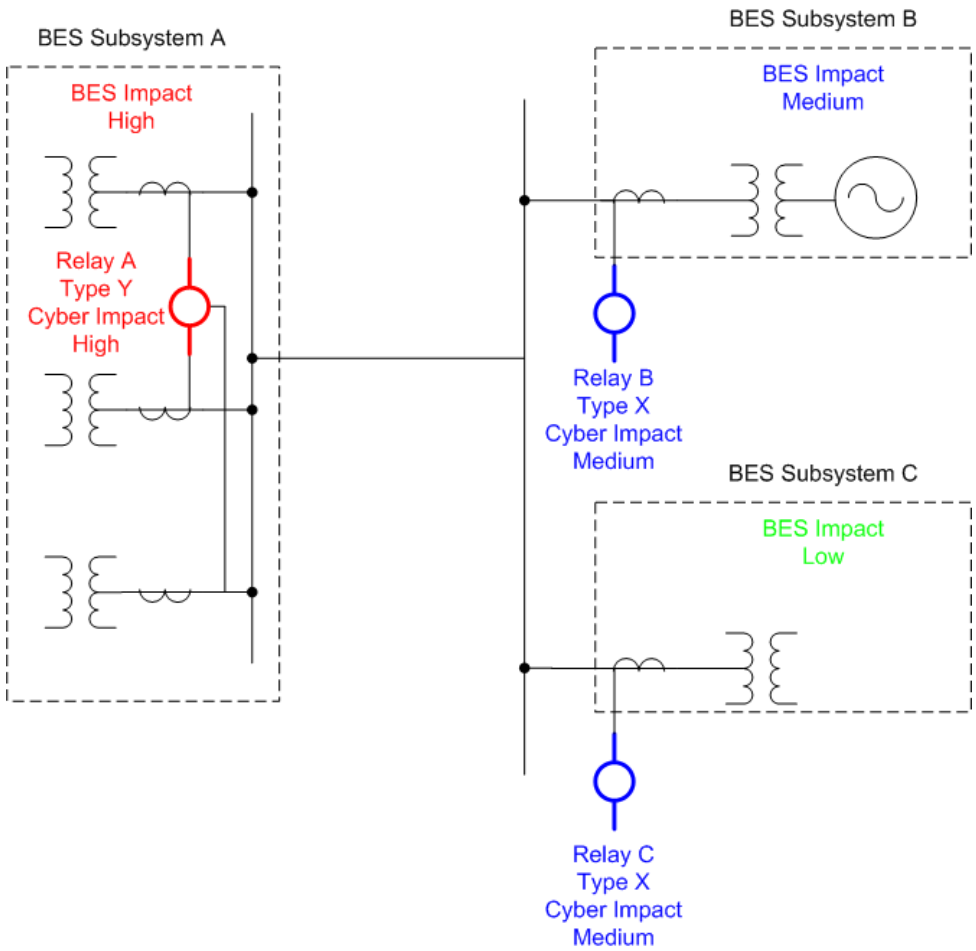
Sample Categorization of Cyber Systems



Example Final Impact Categorization

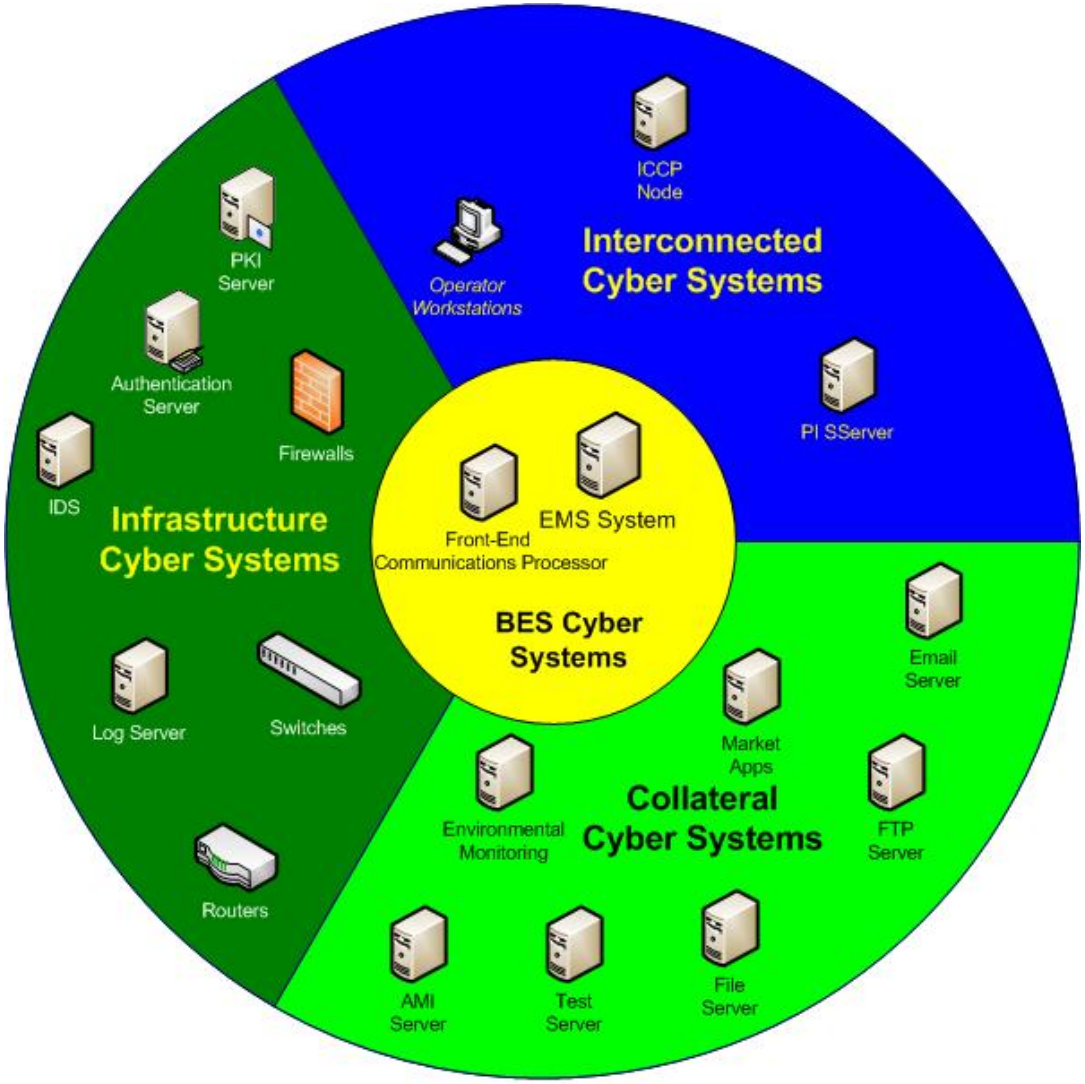
Cyber Impact \ Asset Impact	High	Medium	Low
High	H	H	H
Medium	H	M	M
Low	H	M	L

Final Impact Categorization Diagram



Identical Cyber Systems (Relay X) with the same cyber impact used in the same manner may be ultimately assigned different final categorizations, based on impact of the BES Subsystem they support

Target of Protection



Target of Protection – Control Center

Applying Security Controls

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Apply to *Target of Protection* based on Final Impact Category (High, Medium, Low)
- Develop a library of security controls modeled after NIST 800-53 concepts appropriate to the degree and type of protection needed
- Consider operating environment differences in substations, generating plants and control centers
- Allow flexibility while ensuring adequate protection from dynamic and evolving threats and vulnerabilities

Process Summary

- All Bulk Electric System Subsystems inventoried and mapped to impact categories based on pre-determined criteria
- All Cyber Systems supporting real-time reliability and operability of BES Subsystems inventoried and categorized
- Final Impact Categorization links the Cyber System to the reliability of the BES
- Final product: Categorized list of Cyber Systems to be protected

What's Next

- Standards Drafting Team (SDT) reviews comments to concept paper – September 2009
- SDT drafts CIP-002-3 with consideration of comments (September to December 2009)
  - Help from NERC Operating and Planning Committees members for BES functions and pre-determined engineering impact criteria
- First draft of CIP-002-3 posting for comment: December 2009/January 2010
- SDT continues work on library of security controls and application criteria

Conclusion

- Important step towards a more holistic approach to BES cyber security
- Industry stakeholder input and participation is key for all steps in the standards development from concept paper to final version and implementation plan
- Remember: Industry Comments on the Concept Paper are due on September 4, 2009.

(http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html)

Question & Answer

Contacts:

Joe Bucciero
Project Manager
joe.bucciero@gmail.com
(267) 981-5445

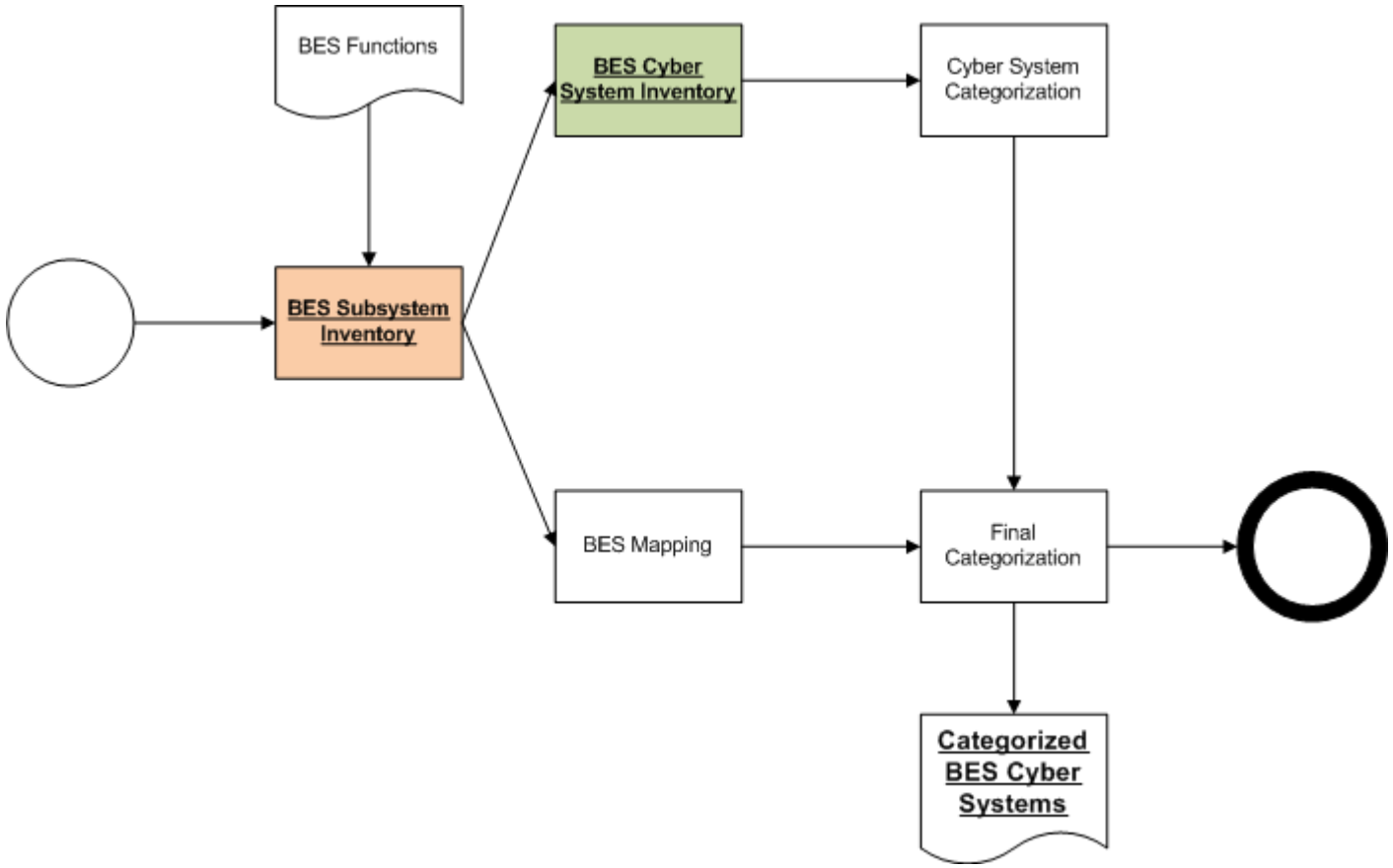
NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

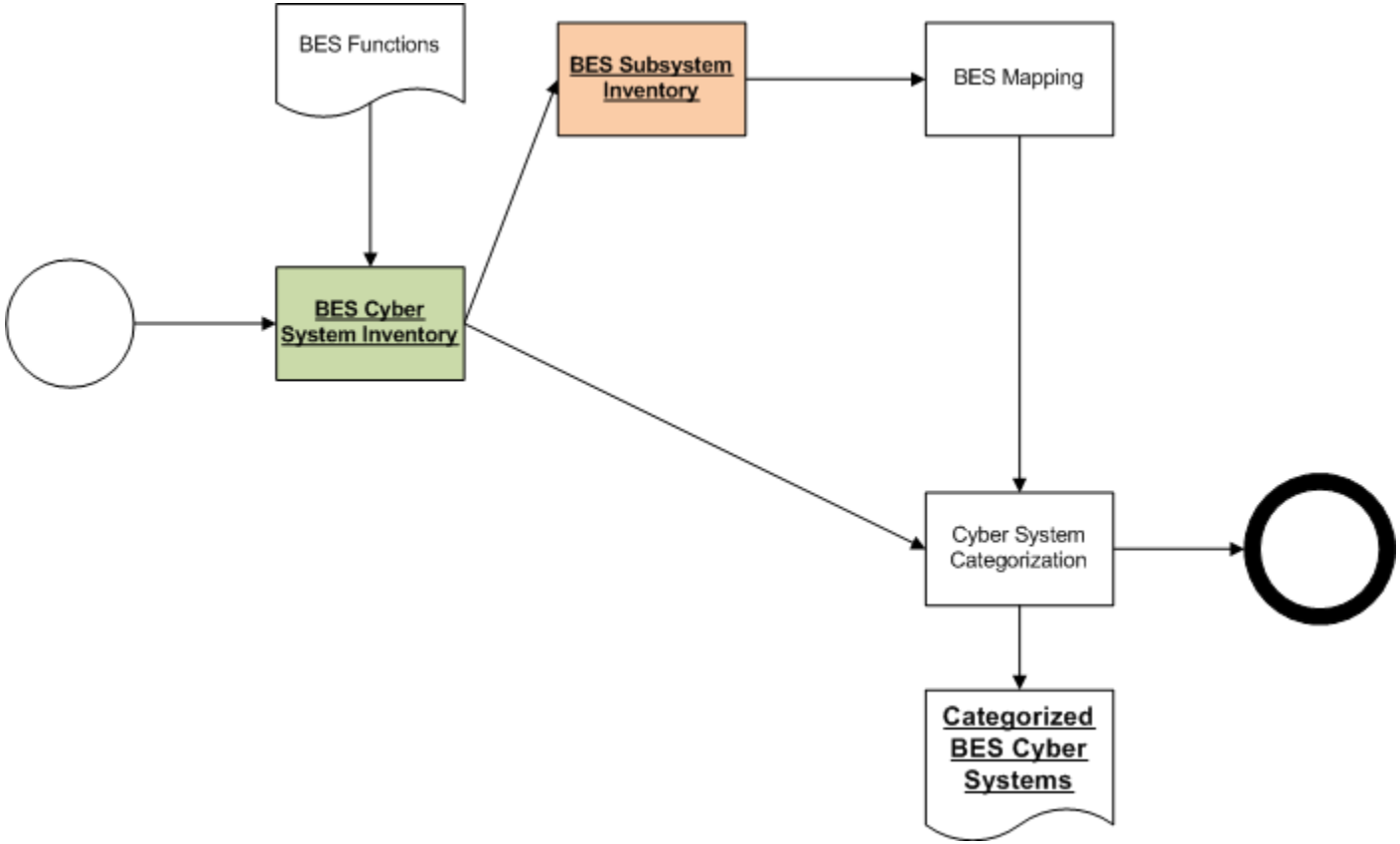
Supplemental Slides for Q&A

to ensure the reliability of the bulk power system

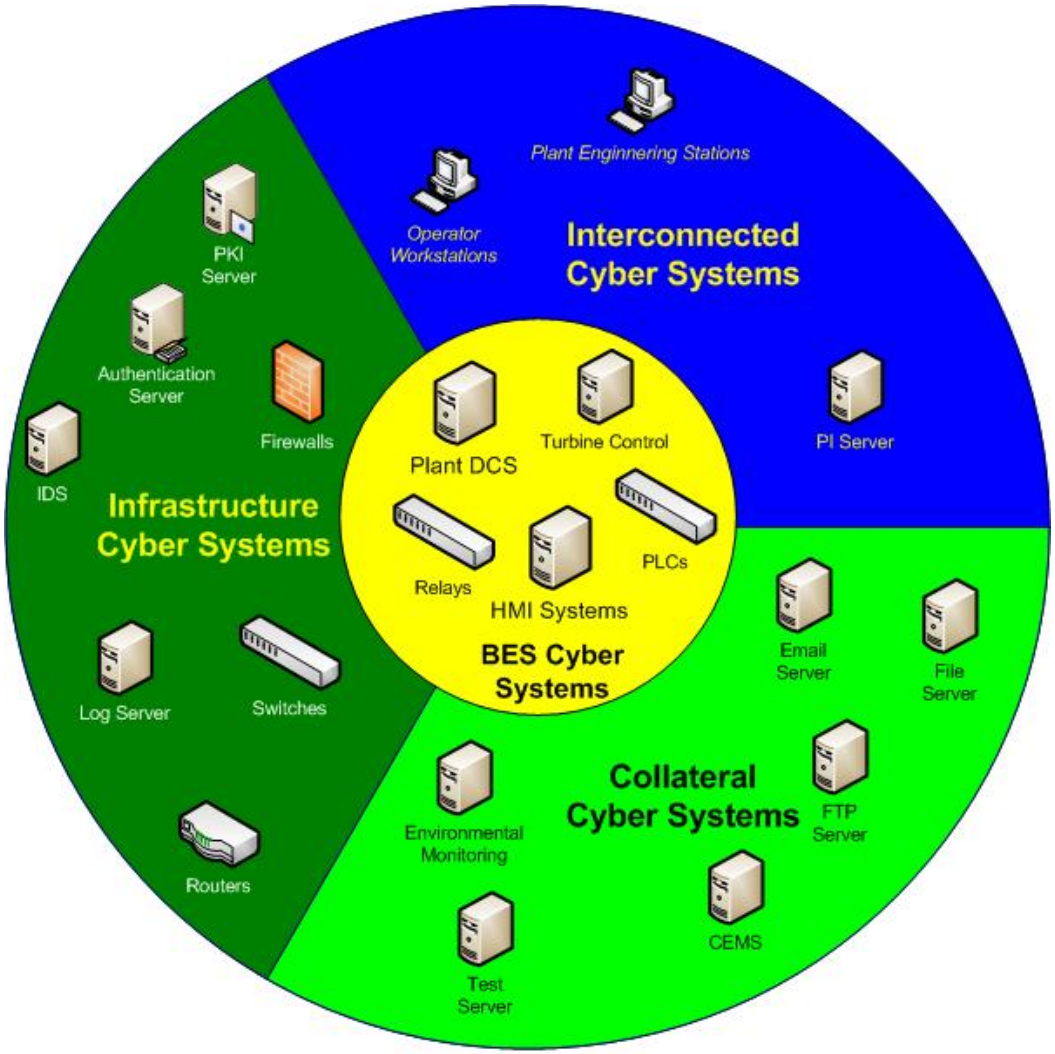
Summary Process Diagram (1/2)
BES Subsystem Centric



Summary Process Diagram (2/2) Cyber System Centric

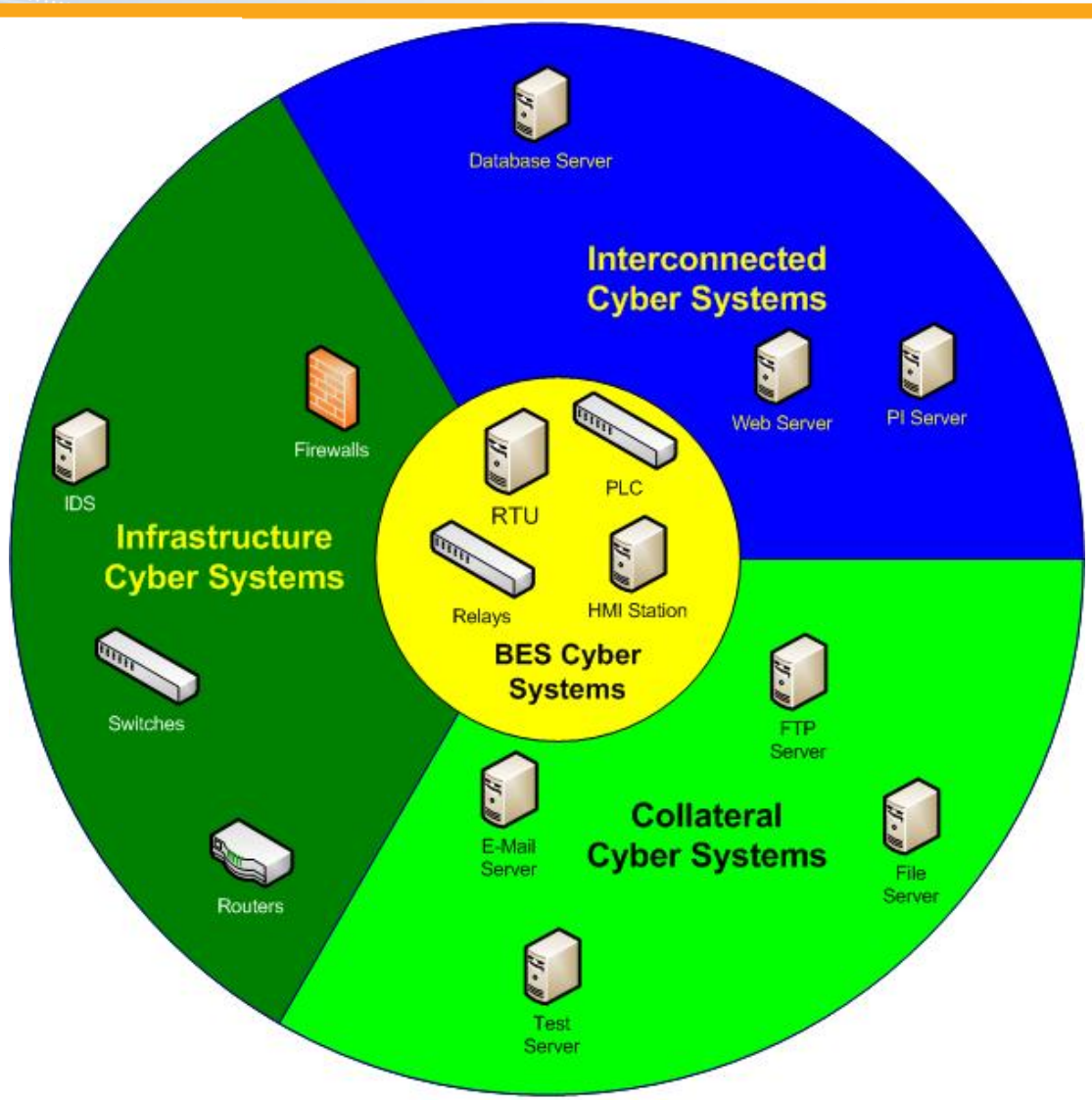


Target of Protection – Generation



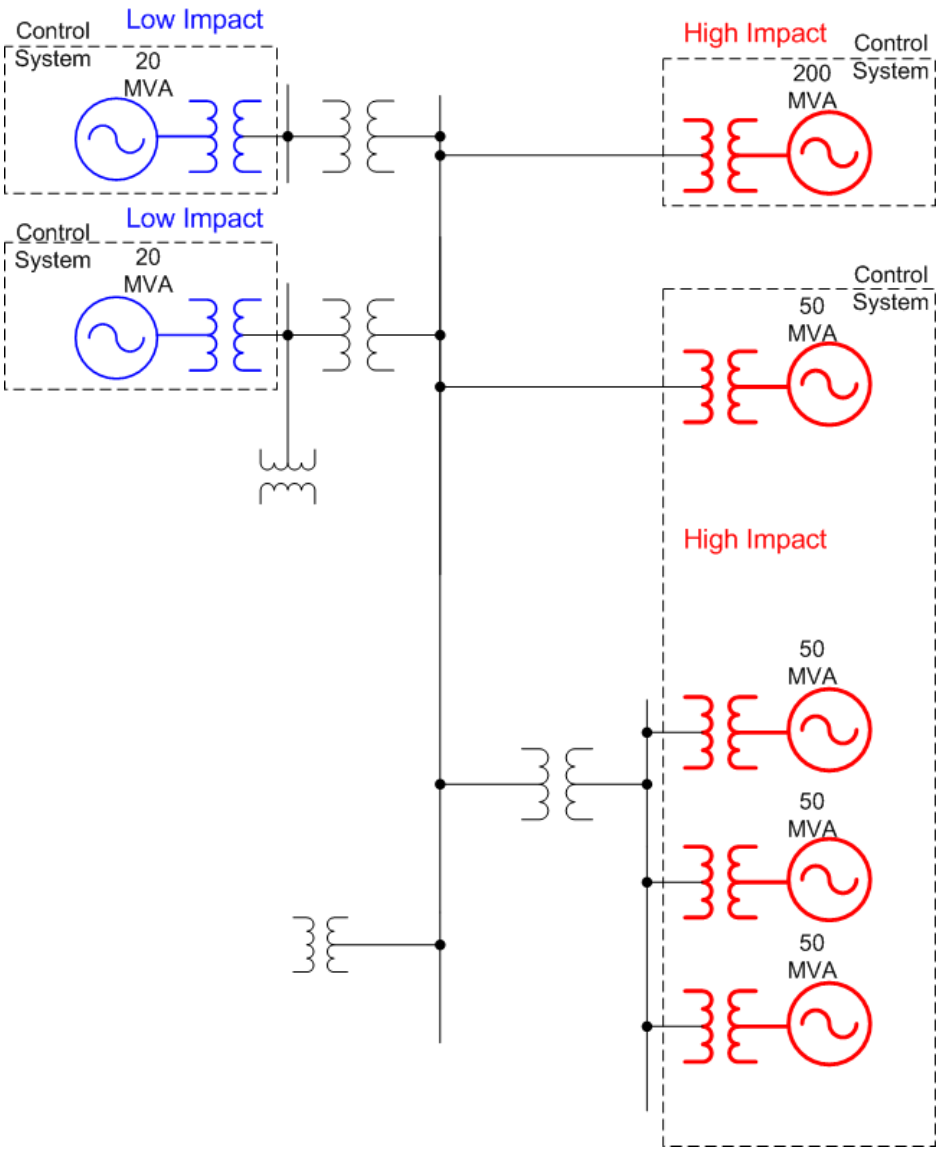
Target of Protection – Generation

Target of Protection – Substation



Target of Protection – Transmission Substations

Reliability Impact of Cyber Systems



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4 Informal Review

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the link below to submit comments on the proposed CIP-002-4. Comments must be submitted by **February 12, 2009.** If you have questions please contact Joe Bucciero at joe.bucciero@gmail.com or by telephone at (267) 981-5445.

Background Information:
FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Some of the modifications were straightforward. Other changes included in Order 706, such as modification to the scope of assets covered by the standard and consideration of the NIST framework, are more complex and require additional consideration. A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008, to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. The SDT for Project 2008-06 has been assigned the responsibility to review each of the CIP cyber security reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706.

Due to the wide variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase strategy to revise the CIP Standards. The initial phase of the project modified the CIP Standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706. The SDT's work in this initial phase resulted in Version 2 of the CIP standards. The NERC Board of Trustees approved Version 2 of the CIP Standards on May 6, 2009. On September 30, 2009 the Commission approved Version 2 of the CIP Reliability Standards for FERC jurisdictional entities.

In addition to approving the Version 2 CIP Standards, the Commission directed NERC to make additional changes to two of the standards (CIP-006-2 and CIP-008-2), the associated implementation plan and to file the modified standards and implementation plan within 90 days. On October 7, 2009, the Standards Committee approved the Standard Authorization Request (SAR) for Project 2009-21 Cyber Security Ninety-day Response. Although the Commission directed changes to only two of the eight (CIP-002-2 thru CIP-009-2) reliability standards, conforming changes were necessary and were drafted for the remaining six CIP Reliability Standards (CIP-002-2 through CIP-005-2, CIP-007-2, and CIP-009-2) to correct the cross references within the set of standards. The initial ballot for CIP-002-3 through CIP-009-3, an implementation plan for Version 3 of the CIP standards, and a supplemental *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* was held from November 20 to November 30, 2009. A recirculation ballot was completed on December 14, 2009. The output of this work became Version 3 of the CIP Reliability Standards. Version 3 CIP standards were approved by the NERC Board of Trustees on December 16, 2009 and will be submitted to FERC for approval by December 29, 2009 in accordance with the FERC 90-day directive.

The Standard Drafting Team is now considering Version 4 of the CIP Reliability Standards, addressing the FERC Order 706 cyber security directed modifications that may require industry discussion. Four key principles are guiding the drafting team's work on these standards:

- Build on work already done to comply with Version 1 of the CIP reliability standards, including the industry's experience and investments
- Address the complex nature of the BES reliability functions and interconnected Cyber Systems, both within and between multiple organizations
- Provide Responsible Entities with reasonable flexibility in applying equivalent security controls on the basis of compensating controls, cyber system characteristics, and operating environment considerations
- Include all Cyber Systems with potential to adversely impact the reliability of the BES if lost, comprised, or rendered unavailable

The SDT initially focused on revising CIP-002 since it establishes the foundation for cyber security protection of the BES. The subsequent cyber security standards establish the baseline cyber security controls that must be implemented to protect the assets identified in CIP-002. The drafting team has prioritized its work in response to Commission and industry concerns regarding identification of assets in CIP-002-1. Work on the remaining cyber security standards is scheduled to begin in January 2010. Drafts of the new standards are anticipated to be posted for industry feedback by July 2010.

Summary of CIP-002 Modifications

A new approach is proposed in draft standard CIP-002-4 — Cyber Security — BES Cyber System Categorization. In collaboration with representatives of the Operating Committee and Planning Committee, the drafting team developed criteria for evaluating the potential level of impact on functions critical to the reliable operation of the BES. The criteria are organized in high, medium, and low BES impact categories. Responsible Entities apply the criteria to map their identified BES Subsystems to BES impact categories. For each BES Cyber System, Responsible Entities assign the highest impact level of the associated BES Subsystem(s).

The Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial draft of CIP-002-4 — Cyber Security — BES Cyber System Categorization. Industry feedback gathered will be used by the drafting team to refine the draft standard for formal industry review in March 2010.

***Please use the electronic comment form to submit your final responses to NERC.**

Questions:

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

   1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

Comments:

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

☐ Agree with proposed definition

☐ Disagree with proposed definition

Comments:

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures.

or

- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures;

or

- could hinder restoration to a normal condition.

☐ Agree with proposed definition

☐ Disagree with proposed definition

Comments:

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

☐ Agree with proposed definition

☐ Disagree with proposed definition

Comments:

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could **not:**

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

☐ Agree with proposed definition

☐ Disagree with proposed definition

Comments:

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

   ☐ Prefer method proposed in the standard

   ☐ Prefer alternative method of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1.

Comments:

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*.

   1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

   1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."

   Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

   2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)

   2.2 The Responsible Entity name

   2.3 The BES impact categorization level"

   Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

☐ Agree

☐ Disagree

Comments:

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

☐ Agree with VRFs

☐ Disagree with VRFs

Comments:

☐ Agree with VSLs

☐ Disagree with VSLs

Comments:

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria?

Suggestions for improving proposed criteria:

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

Suggested Criteria for Load Serving Entities:

Suggested Criteria for Transmission Service Providers:

Suggested Criteria for Interchange Coordinators:

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

    Suggested criteria for NERC and Regional Entities:

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?

    Comments on adding Distribution Provider:

    Comments on adding Reliability Assurer:

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

    Suggestions for improving proposed functions:

13. Do you have any other comments to improve the draft standard?

    Other Comments not already provided in response to earlier questions:

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT
Guidance for the Electric Sector: Categorizing Cyber Systems

to ensure the reliability of the bulk power system

December 2009

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Table of Contents

Introduction 3
The Purpose of Categorizing BES Cyber Systems 3
Criteria for Impact Mapping of BES Subsystems 4
Acknowledging NIST's Risk Management Framework 5
The role of this guidance 7
Categorizing BES Cyber Systems 7
Step 1: Performing a BES Subsystem Inventory 7
Step 2: Categorizing BES Subsystems 8
Step 3: Performing a BES Cyber System Inventory 8
Profiling BES Functions with Respect to Cyber Systems 8
Step 4: Perform an Impact Categorization for each BES Cyber System 9
Step 5: Monitoring for Changes to the System 10

Introduction

Critical infrastructure provides the essential services that underpin our society. Among the most important of the essential services is the Bulk Electric System (BES), which includes the capabilities of generation and transmission of electricity throughout North America. The industry, through NERC, has gone through the continuous refinement of the Cyber Security Standards since 2003 with the first mandatory set of standards approved by FERC on January 18, 2008 in FERC Order 706. This refinement has lead to several revisions of the standards. As the standards have evolved, they had moved from an approach of "one size fits all," to one that is better aligned with a strategy of risk management, with the goal of prioritizing the protection of Cyber Systems based on their potential impact on the BES and applying security controls appropriate to that potential impact.

The Purpose of Categorizing BES Cyber Systems

Having multiple impact categories for BES Cyber Systems will result in the application of more appropriate security controls across a broader spectrum of assets. To accomplish this, the NERC CIP Cyber Security Standards take a functions-based approach as a means to measure impact a particular Cyber System component has to the BES. Attachment 2 of CIP-002-4 identifies several functions as a set of activities that utilities perform to maintain BES reliability. BES Cyber Systems need to be "secure" – not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions. The functions necessary to maintain BES reliability represent a path by which utilities can identify which of their Cyber Systems are essential to or can adversely impact the BES.

Ultimately, the impact-based categorization approach has the purpose of reducing risk to the performance of functions. Hazards to the Cyber System can have an impact to the functions being performed and the security constraints of the Cyber System should reflect this. For example, a generating unit designated as Reliability "must run" could imply a 24x7 availability constraint for the generation control system. Likewise, the selection of security controls should reflect the assurance needed in meeting this constraint. This relationship is shown in Figure 1. The degrees to which a Cyber System can impact the reliable operation of the BES establish the type and amount of security controls that are necessary.

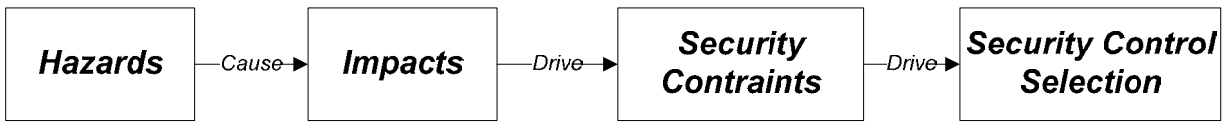


Figure 1: Connecting Avoidance of Hazards to selection of Security Controls

Criteria for Impact Mapping of BES Subsystems

Attachment 1 of CIP-002-4 lists categorization criteria which detail characteristics of BES Subsystems having the potential to impact the BES. The criteria have their basis in impact thresholds associated with BES functions and are patterned after criteria used in categorizing bulk power events. A ***High*** threshold indicates BES Subsystems, which if compromised or rendered unavailable, would significantly affect the integrity of BES system operations. A ***Medium*** threshold indicates BES Subsystems, which if compromised or rendered unavailable, would directly affect the capability of the BES. The ***Low*** category applies to all other BES Subsystems.

These thresholds are defined to provide a straightforward and objective path for a utility to determine the impact categorization of its BES Subsystems. The alignment of potential impacts to BES Subsystems enables a categorization of the inventory of assets relative to potential impact, resulting in a prioritized list of assets that must be protected to ensure the reliability of the BES.

The Cyber Systems which support the functions being performed by the BES Subsystem inherit the impact category. With this categorization of impact, it is possible to evaluate the BES Cyber Systems to determine where they fall on the scale in Figure 2. Consequently, industry resources can be more effectively used to apply the most protection on the smaller number of Cyber Systems with the highest potential impact.

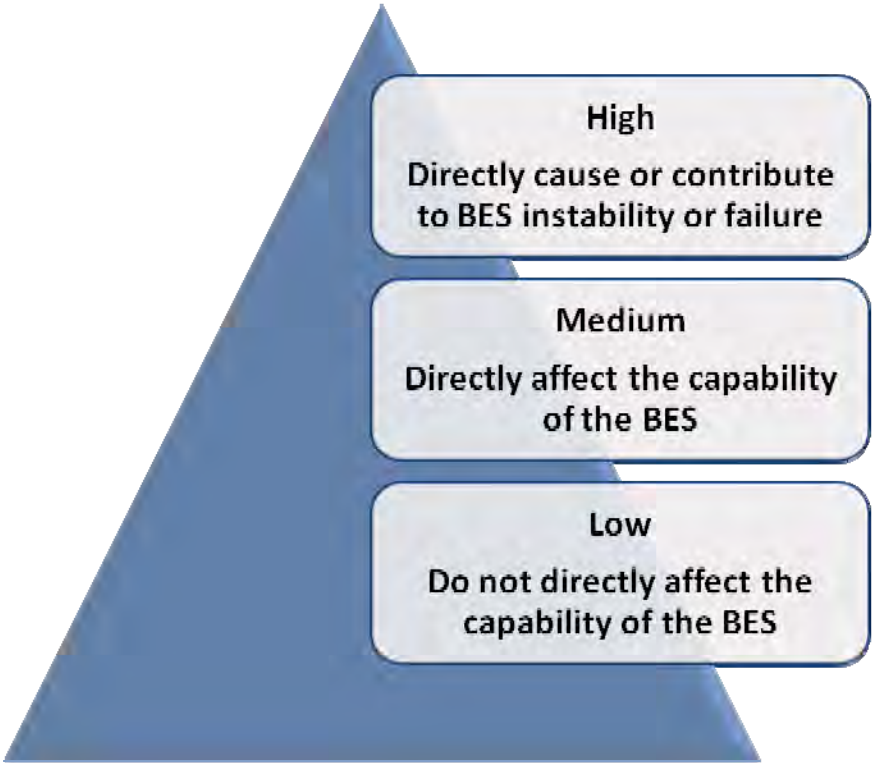


Figure 2: Categorization of BES Cyber Systems

Acknowledging NIST's Risk Management Framework

The CIP-002-4 approach has considered various security risk management frameworks including the NIST Risk Management Framework as an approach to guide utilities in safeguarding the BES. There are many valuable lessons to be learned within the NIST Framework and a number of similarities between it and the NERC CIP Cyber Security Standards.

The NIST Framework involves a continuous process of six discrete steps to categorize and protect information systems. The NERC CIP Cyber Security Standards approach is similar in that it is a continuous process of separate steps for identifying Cyber Systems that support BES functions,

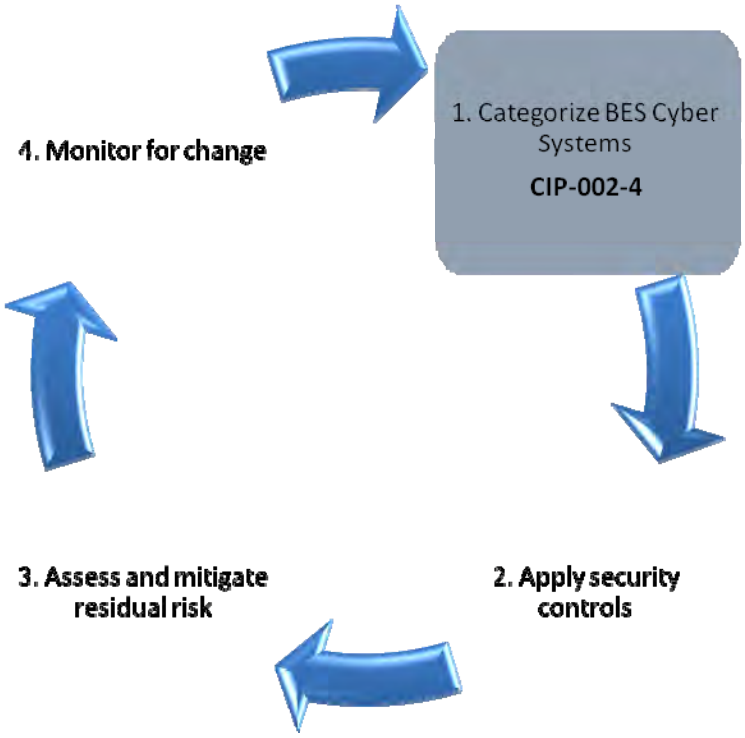


Figure 3: NERC Cyber Security Standards – Security Management Cycle

categorizes Cyber Systems based upon their potential impact to the functions, and assigns security controls based upon that categorization.

It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences is the divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost two hundred different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of functions that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework, as a higher degree of definition of

Cyber Systems and their potential impact to BES functions should yield better fidelity in selection of protection strategies, resulting in a more appropriate investment of resources by utilities.

The role of this guidance

This guidance document serves to assist NERC Registered Entities in categorizing their BES Cyber Systems based on their impact to the reliable operation of the Bulk Electric System.

Categorizing BES Cyber Systems

In this section, a five-step process is outlined to assist entities in categorizing their BES Cyber Systems. This is only one approach, and an entity may choose an alternate approach to complying with the requirements of CIP-002-4. However, this process attempts to build upon the investment utilities may have already made in complying with previous versions of the CIP Standards by utilizing the inventory and categorization of BES Subsystems to categorize their BES Cyber Systems.

Step 1: Performing a BES Subsystem Inventory

The categorization of BES Subsystems in steps 1 and 2 provides a measure of the impact its associated BES Cyber Systems have on the Bulk Electric System.

The inventory of BES Subsystems should include all Generation Subsystems, Transmission Subsystems, and Control Centers owned by the entity. The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. For example, a multiple unit generation facility can be defined as one or more Generation Subsystems depending on the functions being performed and the operational and technical characteristics of the generating units.

The entity should consider any associated BES Cyber Systems when performing the inventory and defining boundaries of BES Subsystems. Although a full BES Cyber System inventory may not be available at this step in the process, the BES Cyber System will ultimately drive the final characterization of the BES Subsystem.

What is a BES Cyber System?

A BES Cyber System is defined in the NERC Glossary as "*a Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System*."

This definition includes all of the components necessary to ensure the protection of the reliability function(s) being performed. To determine these components, the Responsible Entity should consider the following:

1. Primary components – devices performing or having direct impact to the reliability function(s).
2. Interconnected components – servers and workstation components involved in the exchange and display of data associated with the reliability function(s) (e.g., historical data collectors, ICCP nodes, operations support workstations, etc.).
3. Infrastructure support components – devices supporting the confidentiality, integrity, and availability constraints of the BES Cyber System which may be defined by the selection of security controls (e.g., routers, switches, firewalls, access-control servers, security event monitoring servers, virtual server management, etc.)
4. Collateral components – devices included only on their location within a network segment that could be utilized to attack the supported function of the BES Cyber System.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System or they might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

The shared elements that an associated BES Cyber System can impact should be included as part of the BES Subsystem.

Step 2: Categorizing BES Subsystems

Identified BES Subsystems are then mapped into impact categories based on pre-defined criteria in Attachment 1 of CIP-002-4, which reflect their impact on the reliability and operability of the BES. The criteria represent impact thresholds based on the functions identified in Attachment 2 of CIP-002-4.

All BES Subsystems will have an assigned impact category. BES Subsystems that do not meet the High or Medium threshold criteria are by default categorized as Low impact.

Step 3: Performing a BES Cyber System Inventory

The inventory of BES Subsystems can be used as a starting point for identifying BES Cyber Systems. This process involves looking at each of the associated BES functions and determining which Cyber Systems are involved. Each BES Subsystem performs one or more functions of the BES. The identification of these functions provides the basis by which to identify, categorize, and protect BES Cyber Systems.

Profiling BES Functions with Respect to Cyber Systems

The exercise of profiling BES functions is a useful approach to determining BES Cyber Systems. BES functions are defined generically and each Responsible Entity will perform these differently using different components. The task of profiling BES functions involves describing how they are performed and the Cyber Systems that support or impact their performance. The description can be written in non-technical language and should be as specific as possible. This brings the generic function description to a level where the Responsible Entity can identify the function as processes within its operation. Table 1 shows an example profiling of the Reliability Function, Control, and Operation for an entity.

Reliability Function: Control & Operation	Control & Operation includes those activities, actions and conditions that provide monitoring and control of BES elements
Description	Relays and RTUs located at Company X substations provide the SCADA System with status and power flow data. If a protective relay trips at substation Y, then operations personnel are notified through the SCADA alarms or an automated after-hours call-out system. Operations personnel will then assess the condition and issue breaker control to reestablish power to the affected line.

Table 1: Profile of the Reliability Function Control & Operation

The profile can be further represented as a series of process steps that display the Cyber Systems involved for each step as shown in Figure 4.

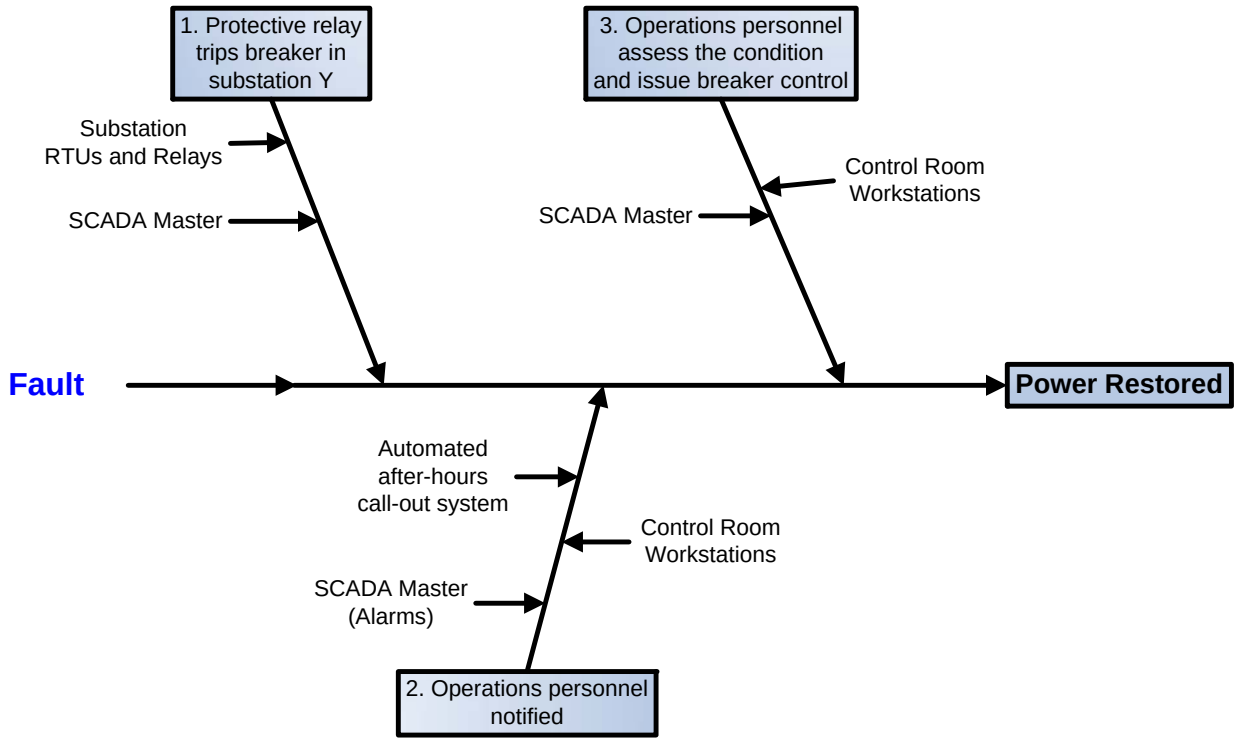


Figure 4: A sample fishbone diagram showing Cyber Systems involved in the function of Control & Operation

Step 4: Perform an Impact Categorization for each BES Cyber System

Using the Cyber System components identified in the previous step, BES Cyber System components can be identified as having the potential to adversely impact the BES function. The Responsible Entity should consider the impact to the Reliability Function given the loss, degradation, and compromise of the Cyber System component. For a complete assessment, each scenario of loss, degradation and compromise of the Cyber System component should be considered individually.

Loss of the BES Cyber System – Both BES Subsystems and BES Cyber Systems routinely go offline with no impact to the BES. However, the analysis should go beyond normal operating conditions to consider the impact of losing the Cyber System at an inopportune time and possibly for an extended period of time.

Degradation of the BES Cyber System – In this case, the BES Cyber System may still remain online but its performance is affected. This may occur in response to an unauthorized change in the system such as a defective upgrade or flood of network packets.

Compromise of the BES Cyber System – Unauthorized, unintended, or malicious use of the BES Cyber System. Specifically, the Responsible Entity should consider the following scenarios as applicable:

- Issuance of control commands to BES Subsystems
- Modification of configuration settings including operational parameters
- Modification of alarm limits
- Modification of collected or transmitted data

The result of this analysis determines the set of BES Cyber System components that have the capability of impacting the BES functions. The components are then grouped as a single or multiple, distinct BES Cyber Systems. Each BES Cyber System inherits the CIP-002 impact categorization (High, Medium, or Low) of the BES Subsystem through which the Reliability Function is being performed.

In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems.

BES Subsystem	Associated Reliability Function(s)	BES Impact
Primary Control Center	Control & Operation	High
Hydro Plant #1	Balancing Load and Generation	Low
Coal Plant #1	Situational Awareness	Medium
Control Center at Company X	Inter-Entity Coordination and Communication	Low
Resultant Impact Categorization		**High**

Table 2: Example Impact Categorization for a SCADA System

Step 5: Monitoring for Changes to the System

Once a BES Cyber System has been assigned an initial impact categorization, processes should be in place to ensure this categorization continually reflects modifications to the electric system and operational processes of the BES Cyber System components. The following types of changes should be monitored as part of the process of BES Cyber System categorization.

1. Modifications to the BES Subsystems that result in a different impact mapping
2. Additions or modifications to the BES functions being performed by a BES Subsystem
3. Modifications to the Cyber System components performing the BES functions, which may result in the need to identify additional BES Cyber System components

To ensure these categories of changes are captured prior to deployment, an organization might include a quarterly review within their processes to capture any new or upcoming changes to the system.

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008).
2. Revised SAR and response to comments approved by SC (July 10, 2008).
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009).
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)

Proposed Action Plan and Description of Current Draft:

This is the initial draft of Version 4 of the proposed CIP-002 standard and is being submitted to the industry for feedback as part of an informal comment period. Industry feedback will be utilized by the drafting team to refine the draft standard for formal industry review in February 2010.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	March 15, 2010
2. Conduct initial ballot.	May 24, 2010
3. Post response to comments on initial ballot.	June 21, 2010
4. Conduct recirculation ballot.	June 21, 2010
5. Submit standard to BOT for adoption.	To be determined.
6. File standard with regulatory authorities.	To be determined.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

High BES Impact

BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures.

    or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures;

    or

  could hinder restoration to a normal condition.

Medium BES Impact

BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

Low BES Impact

BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could **not**:

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

1. Critical Assets
2. Critical Cyber Assets
3. Cyber Assets

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-4

3. **Purpose:** To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES.

4. **Applicability:**

   4.1. Functional Entities:

   For purposes of the requirements contained herein, the listing of Functional Entities will be collectively referred to as "Responsible Entities." In situations where a specific Functional Entity or subset of Functional Entities are used, the Functional Entity(ies) will be specified explicitly.

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Coordinator.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load-Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

5. **Physical Facilities:**

   5.1. All BES facilities,(including those structures, components, equipment and systems of facilities within a nuclear generation plant not regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission).

6. **Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the eighth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*. (*Violation Risk Factor: High*)

1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1.

R2. To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem(s) for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem: *(Violation Risk Factor: High)*

2.1. Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)

2.2. The Responsible Entity name

2.3. The BES impact categorization level

R3. As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows: *(Violation Risk Factor: High)*

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in *CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System.*

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems.

C. Measures

M1. The Responsible Entity shall have evidence, including its dated categorized list of BES Subsystems, to show that it has a categorized list of BES Subsystems as required by R1.

M1.1. The Responsible Entity shall have evidence that it updated its categorized list, if applicable, within 30 calendar days as a result of the commissioning of any new BES subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric as required by Requirement R1, Part 1.1.

M1.2. For each BES Subsystem where a Responsible Entity uses an engineering analysis or assessment method required by Attachment1, the Responsible Entity shall have evidence, such as a copy of the engineering analysis or assessment method used or a copy of the dated email transmittal, electronic voice recording, or other evidence to show that it received the approval of its Reliability Coordinator or Reliability Assurer for use of that method.

M2. The Responsible Entity shall have evidence of notifications as required by Requirement R2.

M3. The Responsible Entity shall have evidence, including its categorized list of BES Cyber Systems and the associated BES Subsystem impact categorizations as evidence that its BES Cyber Systems have been assigned BES impact categories as required by Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1. Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2. ERO for Regional Entity.

1.1.3. Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Data Retention

Each Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence for Requirements R1 through R3, Measures M1 through M3 for a full calendar year or since the last update, whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant.

The Compliance Enforcement Authority, in conjunction with the Registered Entity, shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Compliance Monitoring and Assessment Processes

1.4.1 Compliance Audits

1.4.2 Self-Certifications

1.4.3 Spot Checking

1.4.4 Compliance Violation Investigations

1.4.5 Self-Reporting

1.4.6 Complaints

1.5. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
1	One or more Low Impact BES Subsystems has not been categorized.	One or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact. OR The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30, but within less than or equal to 40 calendar days of the completion of the change.	One High Impact BES Subsystem has not been categorized or has been miscategorized as Medium or Low Impact. OR The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 40, but within less than or equal to 50 calendar days of the completion of the change.	More than one High Impact BES Subsystems has not been categorized or has been miscategorized as Medium or Low Impact. OR The Responsible Entity failed to update its categorized list of BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 50 calendar days following the completion of the change. OR The Responsible Entity has not categorized any BES Subsystems it owns.
2		The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization level within 31 to 60 days of the categorization.	The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization level within 61 to 90 days of the categorization.	The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization for more than 90 days after the categorization.
3	Five or more Low Impact BES Cyber Systems have not been categorized.	Three or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact.	The Responsible Entity has not assigned an impact category to one High impact BES Cyber System or has miscategorized one High Impact BES Cyber System as Medium or Low Impact.	The Responsible Entity has not assigned an impact category to more than one High impact BES Cyber System or more than one High Impact BES Cyber Systems has been miscategorized as Medium or Low.

				OR The Responsible Entity has not performed and documented a categorization of any of the BES Cyber Systems it owns. OR The Responsible Entity does not have a list of all its BES Cyber Systems.

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
4	12/29/2009	Initial draft of Version 4 Use of new format standard template	

CIP-002 — Attachment 1

Criteria for BES Impact Categorization of BES Subsystems

1. High BES Impact (H)

   1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support, in which case such Subsystems may be categorized as Medium BES Impact.

   1.2. Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations.

   1.3. Each Generation Subsystem that has been pre-designated as Reliability "must run" units.

   1.4. Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan.

   1.5. Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines leaving the station , unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Reliability Assurer, either for voltage or frequency stability support.

   1.6. Each Transmission Subsystem comprising the Cranking Paths.

   1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method.

   1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner.

   1.9. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above.

   1.10. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse as determined through an engineering evaluation or other assessment method.

   1.11. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method.

   1.12. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages.

1.13. Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact.

1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more.

1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions.

1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more.

2. Medium BES Impact (M)

2.1. Each Generation Subsystem with aggregate rated name-plate generation of 1000 MVA or more, not already included in section 1 above, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support.

2.2. Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency stability support.

2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact.

2.4. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001-1 for Medium Impact Nuclear facilities as determined under Criterion 2.1 above.

2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact.

2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above.

3. Low BES Impact (L)

All other BES Subsystems on the list not mapped to Section 1 High BES Impact or Section 2 Medium BES Impact.

CIP-002 — Attachment 2

Functions Critical to the Reliable Operation of the Bulk Electric System

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

1. Dynamic Response

The Dynamic Response function includes those actions performed by BES elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response
- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

2. Balancing Load and Generation

The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of ACE
  - Field data sources (real time tie flows, frequency sources, time error, etc)
  - Software used to perform calculation
- Unit commitment
  - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc) , load schedules
- Load management
  - Ability to identify load change need
  - Ability to implement load changes
- Demand Response
  - Ability to identify load change need
  - Ability to implement load changes
- Manually Initiated Load shedding
  - Ability to identify load change need
  - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time
  - Start units and provide energy

3. Controlling Frequency (real power)

The function of Controlling Frequency includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics
  - Software to calculate unit adjustments
  - Transmit adjustments to individual units
  - Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

4. Controlling Voltage (reactive power)

The function of Controlling Voltage includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage function include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources

  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

5. Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)
- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's
- Identify and monitor Flowgates

6. Control & Operation

Control & Operation includes those activities, actions and conditions that provide monitoring and control of BES elements.

An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches (such as SCADA)

7. Restoration of BES

The Restoration of BES function includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES function include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

8. Situational Awareness

The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness function include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis

- Frequency monitoring

9. Inter-Entity Coordination and Communication

The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication function include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Informal Comment Request

December 29, 2009–February 12, 2010

Now available at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Project 2008-06: Cyber Security Order 706 (Phase II)

The Standard Drafting Team for this project is seeking informal industry feedback and suggestions on the initial draft of CIP-002-4 — Cyber Security — BES Cyber System Categorization **until 8 p.m. EST on February 12, 2010.**

The input will be considered by the drafting team in revising and refining CIP-002-4 requirements and related documents. In the draft *Guidance for the Electric Sector: Categorizing Cyber Systems*, posted with the standard, the drafting team discusses the proposed method for categorizing a BES Cyber System according to its potential impacts on the reliable operation of the BES.

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Next Steps

This informal comment period will be followed by a 45-day formal comment period, which will include the formation of a ballot pool. The initial ballot will begin shortly after the team posts its response to comments. Note that the Standards Committee will allow the drafting team to make modifications to the standard, if needed, between the initial and recirculation ballots. These special steps will help the team meet its schedule for delivery of the set of CIP standards.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 – Cyber Security Order 706. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy.

The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees on May 6, 2009 and FERC on September 30, 2009. As part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards, which were approved by the NERC Board of Trustees on December 16, 2009 and will be submitted to FERC for approval by December 29, 2009.

This phase will result in version 4 of the CIP standards. The drafting team believes CIP-002 and its requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of deliberation and industry input, the SDT is presenting a draft standard CIP-002-4 — Cyber Security — BES Cyber System Categorization that categorizes BES Cyber Systems according to impacts on reliability functions. Work on the subsequent cyber security standards that establish the cyber security controls that must be implemented to protect the assets identified in CIP-002, appropriate to BES impact, is scheduled to begin in January 2010.

Page for Phase II: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html
Main project page for 2008-06: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity
Physical Facilities (see proposed standard)

Proposed Glossary of Terms Changes

New terms:
Cyber System
BES Cyber System
Bulk Electric System Subsystem (BES Subsystem)
Generation Subsystem
Transmission Subsystem
Control Center
High BES Impact
Medium BES Impact
Low BES Impact

Terms to be retired once the standards that use those terms are replaced:
Critical Assets
Critical Cyber Assets
Cyber Assets

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments on Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the draft CIP-002-4 standard. This standard was posted for a 45-day public comment period from December 29, 2009 through February 12, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 107 sets of comments, including comments from more than XX different people from approximately XX companies representing X of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Contro Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification. 16

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data. 16

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. 37

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy. 54

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System. 67

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System. 82

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: 95

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable: 113

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could: 139

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not: 158

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potenial impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement. 175

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method. 193

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria fr BES Impact Categorization of BES Subsystems. ... 212
5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem: ... 246
6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows: ... 261
7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs. ... 279
8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria? ... 294
9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators? ... 333
10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities? ... 345
11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities? ... 351
12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions? ... 362
13. Do you have any other comments to improve the draft standard? ... 374

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Individual	Jennifer Bullock	Progress Energy	X		X		X	X				
2.	Group	Jack Cashin	EPSA					X					
3.	Individual	Greg Mason	Dynegy, Inc					X					
4.	Individual	G. Mark Cole	Georgia System Operations Corporation & Oglethorpe Power Corporation			X	X	X					
5.	Individual	Ernie Hayden	Private Citizen										
6.	Individual	Randy Schimka	San Diego Gas and Electric Co	X		X		X					
7.	Group	Allen Mosher	American Public Power Association										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Eric Olson	Transmission Agency of Northern California	WECC	1
2.	Scott Miller	Municipal Electric Authority of Georgia (MEAG)	SERC	1, 3, 5
3.	Frank Gaffney	Florida Municipal Power Agency (FMPA)	FRCC	1, 3, 5
4.	Virginia Cook	JEA	FRCC	1, 3, 5
5.	Jonathan Appelbaum	Long Island Power Authority	NPCC	1, 3
6.	David Godfrey	Texas Municipal Power Agency (TMPA)	ERCOT	1, 5

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		7. John Allen	City Utilities of Springfield, Missouri	SPP 1, 3, 5									
8.	Individual	Joylyn Stover	Consumers Energy			X	X	X					
9.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gerry Dunbar	Northeast Power Coordianting Council	NPCC	10
3.	Gregory Campoli	New York Independent System Operator	NPCC	2
4.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	2
5.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
6.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
7.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
8.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5
11.	Kathleen Goodman	ISO - New England	NPCC	2
12.	David Kiguel	Hydro One Networks Inc.	NPCC	1
13.	Michael R. Lombardi	Northeast Utilities	NPCC	1
14.	Randy MacDonald	New Brunswick System Operator	NPCC	2
15.	Greg Mason	Dynegy Generation	NPCC	5
16.	Bruce Metruck	New York Power Authority	NPCC	6
17.	Chris Orzel	FPL Energy/NextEra Energy	NPCC	5
18.	Robert Pellegrini	The United Illuminating Company	NPCC	1
19.	Saurabh Saksena	National Grid	NPCC	1
20.	Michael Schiavone	National Grid	NPCC	1
21.	Peter Yost	Consolidated Edison Co. of New York,		3

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
			Inc.										
10.	Group	Tracey Stewart	Southwestern Power Administration	X									
11.	Individual	Shawn Barrett	Michigan Public Power Agency					X					
12.	Individual	Steve Alexanderson	Central Lincoln			X							
13.	Individual	Jian Zhang	TransAlta					X					
14.	Group	Michael Assante	NERC										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Mix	NERC CIP	NA - Not Applicable	
2.	Gerry Adamski	NERC Standards	NA - Not Applicable	
3.	Tim Roxey	NERC CIP	NA - Not Applicable	
4.	Ralph Anderson	NERC CIP	NA - Not Applicable	
5.	Roger Lampila	NERC Compliance	NA - Not Applicable	
6.	Tom Hofstetter	NERC Compliance	NA - Not Applicable	
7.	Todd Thompson	NERC Compliance Investigations	NA - Not Applicable	

15.	Group	Ruth Blevins	Dominon Resources Services, Inc.	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Robert S. Wright	Operations Center	SERC	3
2.	Carl J. Eng	Elec Tran Sys Operations	SERC	1
3.	Joseph R. Finnegan	Elec Tran Sys Operations	SERC	1
4.	Jeff Heffelman	F&H Sys Operations	SERC	5
5.	Matthew Woodzell	F&H Regulatory Compliance	SERC	5
6.	Michael Gildea	Elec Market Policy	NA - Not Applicable	NA
7.	Marvin Walker	IT Support - ET Sys Operations	SERC	1
8.	Steve Edwards	Elec Tran Reliability	SERC	1
9.	Perry Esposito	F&H Engineering	SERC	5

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		10. Chip Humphrey	F&H Merchant Operations	RFC					5				
		11. Fatima Ahmed	F&H Merchant Operations	RFC					5				
		12. Connie Lowe	F&H Market Ops Center	SERC					5				
		13. Marc Gaudette	IT Risk Management	MRO					5				
		14. Charles Bonner	F&H Energy Supply	SERC					5				
		15. John Calder	Elec Tran Compliance	SERC					1				
		16. Vern Colbert	Trans Systems Oper	SERC					1				
		17. John Loftis	Elec Tran Compliance	SERC					1				
		18. Tim Morrissey	Merchant Operations Support	NPCC					5				
		19. Art Bevilacqua	DENE Salem Support	NPCC					5				
		20. Dennis Sollars	IT Compliance	NA - Not Applicable					NA				
		21. Louis Slade	Electric Market Policy	SERC					6				
		22. Mike Garton	Electric Market Policy	MRO					5				
		23. Randy Reynolds	Elec Tran Substation Eng	SERC					1				
		24. George Wood	Elec Tran Substation Ops	SERC					1				
		25. Ronnie Bailey	Elec Tran Planning	SERC					1				
16.	Group	Matt Luallen	Encari								X		
		Additional Member	**Additional Organization**	**Region**					**Segment Selection**				
		1. Mark Simon	Encari	NA - Not Applicable					8				
		2. Peter Brown	Encari	NA - Not Applicable					8				
		3. Steve Hamburg	Encari	NA - Not Applicable					8				
		4. Lenny Mansell	Encari	NA - Not Applicable					8				
		5. Justin Harvey	Encari	NA - Not Applicable					8				
17.	Individual	Karl Bryan	US Army Corps of Engineers, Northwestern Division	X				X					
18.	Individual	Patrick Farrell	Southern California Edison Company	X		X		X	X				
19.	Individual	Martin Bauer	US Bureau of Reclamation					X					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
20.	Group	Ron Blume	Dyonyx										
21.	Individual	Thomas E Washburn	FMPP		X								
22.	Group	Jason Marshall	Midwest ISO		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Mason	Dynegy	NPCC	5
2.	John Alberts	Wolverine Power Cooperative	RFC	1
3.	Barb Kedrowski	We Energies	RFC	3, 4, 5
4.	Lee Kittelson	Otter Tail Power	MRO	1
5.	Bill Hutchison	SIPC	SERC	1, 3, 4, 5
6.	Michael Ayotte	ITC	RFC	1
7.	Randi k. Woodward	Minnesota Power (ALLETE, Inc.)	MRO	1
8.	Joe Knight	Great River Energy	MRO	1, 3, 5, 6

23.	Individual	Bo Jones	Westar Energy	X		X		X	X				
24.	Individual	Green Country Energy	Green Country Energy					X					
25.	Individual	Jerome (Jerry) Murray	Oregon PUC Safety Reliability Security Staff									X	
26.	Individual	Kevin Calhoun	NB Power Generation					X					
27.	Individual	Tony Weekes	MB Hydro (Manitoba 1)	X									
28.	Individual	John Alberts	Wolverine Power Supply Cooperative, Inc	X		X		X	X				
29.	Individual	Mike McClain	Portland General Electric (Portland GE)	X		X		X	X				
30.	Group	Chris Klemm	Public Service Enterprise Group Companies (PSEG)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Robert N Green	PSE&G	RFC	1, 3
2.	David Murray	PSEG Fossil, LLC	RFC	5

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		3. Clint Bogan	PSEG Power CT, LLC	NPCC			5						
		4. Dominic DiBari	Odessa Power Partners, LLC	ERCOT			5						
		5. James Hebson	PSEG Energy Resources and Trade, LLC	RFC			6						
31.	Individual	William Lucas	Wisconsin Electric Power Company (WE-Energies)			X		X					
32.	Individual	Mike Hendrix	Idaho Power Company	X		X		X					
33.	Group	Stephen Mizelle	Southern Company Services, Inc. (SOCO)	X									
		Additional Member	**Additional Organization**	**Region**			**Segment Selection**						
		1. Marc Butts	Southern Company transmission	SERC			1						
34.	Group	Mark Stefaniak	Detroit Edison (DTE)			X		X					
		Additional Member	**Additional Organization**	**Region**			**Segment Selection**						
		1. Mark Stefaniak	Detroit Edison	RFC			3, 5						
		2. Chris Plensdorf	Detroit Edison	RFC			3, 5						
		3. Brian Schulte	Detroit Edison	RFC			3, 5						
		4. Tom Kopera	Detroit Edison	RFC			3, 5						
35.	Individual	James H. Sorrels, Jr	American Electric Power (AEP)	X		X		X	X				
36.	Individual	John Falsey	Edison Mission Marketing and Trading					X					
37.	Individual	Rob Burt	Capital Power Corporation					X					
38.	Individual	Roger Fradenburgh	Network & Security Technologies Inc (NS&T)								X		
39.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X							
40.	Group	Brent Ingebrigtson	E ON U.S,	X		X		X	X				
41.	Individual	Kevin Emery	Carthage Water and Electric Plant			X							
42.	Individual	Louise McCarren	Western Electricity Coordinating Council										X
43.	Individual	Dave Norton	Entergy	X		X		X					
44.	Individual	John Brockhan	CenterPoint Energy Houston Electric	X		x							

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
45.	Individual	Don Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition (CA Cogen)										
46.	Individual	Dave Sutherland	LCRA Transmission Services Corporation	X									
47.	Individual	Linda Campbell	FRCC										X
48.	Individual	Tim Conway	Northern Indiana Public Service Company (NIPSCO)	X		X		X	X				
49.	Individual	Christopher L. de Graffernied, Sr.	on behalf of Consolidated Edison Co. of NY, Inc. and Orange & Rockland Utilities (ConEd)	X		X		X	X				
50.	Group	David Batz	EEI										
51.	Individual	Edward Bedder	Orange and Rockland Utilities Inc (O&R)	X		X							
52.	Individual	Kenneth A Goldsmith	Alliant Energy				X						
53.	Individual	Kirt Shah	Ameren	X		X		X	X				
54.	Individual	Bob Case	Black Hills Corporation	X		X	X	X	X				
55.	Individual	Trevor Tidwell	Texas-New Mexico Power Company (TNMP)	X									
56.	Individual	Richard Salgo	Sierra Pacific d/b/a NV Energy	X									
57.	Individual	E. Hahn	MWDSC	X						X			
58.	Individual	Fed Meyer	The Empire District Electric Company	X		X		X					
59.	Individual	Gary Ofner	North Carolina Electric Membership Corporation (NCEMCS)			X	X	X					
60.	Individual	Gordon Rawlings	British Columbia Transmission Corp. (BCTC)	X	X								
61.	Individual	James jones	Southwest Transmission Cooperative, Inc. (SWTC)	X									
62.	Individual	James Sharpe	South Carolina Electric and Gas (SCEG)	X		X		X	X				
63.	Individual	John Blazekovich	Exelon	X		X		X					
64.	Group	Denise Koehn	Bonneville Power Administration,	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
			Transmission Reliability Program (BPA Trans)										
			Additional Member / **Additional Organization** / **Region** / **Segment Selection**										
			1. Curt Wilkins — BPA Transmission, System Operations — WECC — 1										
			2. Kelly Hazelton — BPA Transmission, System Operations — WECC — 1										
			3. Dick Winters — BPA Transmission, Substation Operations — WECC — 1										
			4. Kevin Dorning — BPA Transmission, PSC Technical Services — WECC — 1										
			5. Tom Gist — BPA Transmission, CC HW Dsgn/Stds Montr & Admin — WECC — 1										
			6. Sharon Brown — BPA Transmission, Project and Planning Support — WECC — 1										
			7. Mike Viles — BPA Transmission, Technical Operations — WECC — 1										
			8. Kevin Carman — BPA Transmission, Planning & Asset Management — WECC — 1										
			9. Rita Coppernoll — BPA Transmission, SPC Technical Svcs — WECC — 1										
			10. Deanna Phillips — BPA, FERC Compliance Office — WECC — 1, 3, 5, 6										
			11. John Wylder — BPA Transmission, CC HW Dsgn/Stds Montr & Admin — WECC — 1										
			12. James Phillips — BPA Transmission, System Operations — WECC — 1										
65.	Individual	Roger Champagne	Hydro-Québec TransÉnergie (HQT)	X									
66.	Individual	Chris Lyons	Constellation Energy Commodities Group (CCG)			X							
67.	Individual	Robert K. Loy	Allegheny Energy Supply Company, LLC (Allegheny Supply)					X					
68.	Group	Michael Gammon	Kansas City Power & Light (KCPL)	X		X		X	X				
			Additional Member / **Additional Organization** / **Region** / **Segment Selection**										
			1. Jennifer Flandermeyer — KCPL — SPP — 1, 3, 5, 6										
			2. Todd Fridley — KCPL — SPP — 1, 3, 5, 6										
69.	Group	Kara Dundas	Conectiv Energy Supply, Inc.					X	X				
70.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
71.	Group	Terrence Simon	Constellation Energy (Constellation Power Generation, Inc.) (CPG)					X					
72.	Group	Terry L. Blackwell	South Carolina Public Service Authority (Santee Cooper)	X									

	Additional Member	Additional Organization	Region	Segment Selection
1.	S. T. Abrams	Santee Cooper	SERC	1
2.	Glenn Stephens	Santee Cooper	SERC	1
3.	Jim Peterson	Santee Cooper	SERC	1
4.	Rene' Free	Santee Cooper	SERC	1
5.	Vicky Budreau	Santee Cooper	SERC	1
6.	Wayne Ahl	Santee Cooper	SERC	1

73.	Individual	Larry Saxon	OGE Energy Corp	X		X		X					
74.	Individual	Darryl Curtis	Oncor Electric Delivery LLC	X									
75.	Group	Mark Heimbach	PPL Supply (PPL Generation & PPL EnergyPlus)					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	James Batug	PPL Generation	RFC	5
2.	Annette Bannon	PPL Generation	NPCC	5
3.	Mark Heimbach	PPL EnergyPlus	RFC	6

76.	Group	Jared Shakespeare	City of St. George			X		X				X	
77.	Individual	Saurabh Saksena	National Grid (NGRID)	X		X							
78.	Individual	Joseph DePoorter	Madison Gas and Electric Company (MGE)			X	X	X	X				
79.	Group	Doug Hohlbaugh	FirstEnergy Corp. (FE)	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rob Martinko	FirstEnergy	RFC	1, 3, 4, 5, 6

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
80.	Individual	Ron Donahey	Tampa Electric Company (TECO)	X		X		X	X				
81.	Individual	Ramona Marino	Snohomish County PUD				X						
82.	Individual	CJ Ingersoll	Constellation (CECD)										
83.	Group	Carol Gerou	Midwest Reliability Organization (MRO)										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tom Webb	WPS	MRO	3, 4, 5, 6
2.	Terry Bilke	Midwest ISO Inc.	MRO	2
3.	Jodi Jenson	Western Area Power Administration	MRO	1, 6
4.	Ken Goldsmith	Alliant Energy	MRO	4
5.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6
6.	Eric Ruskamp	Lincoln Electric System	MRO	1, 3, 5, 6
7.	Joseph Knight	Great River Energy	MRO	1, 3, 5, 6
8.	Joe DePoorter	Madison Gas & Electric	MRO	3, 4, 5, 6
9.	Scott Nickels	Rochester Public Utilties	MRO	4
10.	Terry Harbour	MidAmerican Energy Company	MRO	1, 3, 5, 6

84.	Individual	Anthony Wright	Georgia Transmission Corporation (GTC)	X									
85.	Individual	Jon Kapitz	Xcel Energy	X		X		X	X				
86.	Individual	Alan Gale	City of Tallahassee					x					
87.	Individual	Bill Keagle	GBE	X									
88.	Individual	John Allen	City Utilities of Springfield, Missouri	X									
89.	Group	Silvia Parada Mitchell	Florida Power & Light (FPL)	X		X		X	X				
90.	Group	William J. Gallagher	Transmission Access Policy Study Group (TAPS)										
91.	Individual	William J. Smith	Allegheny Power	X									
92.	Individual	Frank Gaffney	Florida Municipal Power Agency (FMPA)			X	X	X	X				
93.	Individual	Greg Rowland	Duke Energy	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
94.	Individual	Randy MacDonald	NBSO		X								
95.	Group	Edvard Lauman	Acumen Engineered Solutions International Inc. (AESI)										
96.	Individual	Dan Rochester	Independent Electricity System Operator (IESO)		X								
97.	Individual	Kasia Mihalchuk	Manitoba Hydro (Manitoba 2)	X		X		X	X				
98.	Individual	Oklahoma Municipal Power Authority	Oklahoma Municipal Power Authority (OMPA)				X						
99.	Individual	Jason Shaver	American Transmission Company (ATC)	X									
100.	Individual	Eric Ruskamp	Lincoln Electric System (LES)	X		X		X	X				
101.	Individual	Catherine Koch	Puget Sound Energy (PSE)	X									
102.	Group	Scott Berry	Indiana Municipal Power Agency (IMPA)				X						
		Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
		1. Mike Jenner	City of Edinburgh, Indiana	RFC									
103.	Individual	Christine Hasha	ERCOT ISO		X								X
104.	Group	Sandra Shaffer	PacifiCorp	X		X		X	X				
105.	Group	Ben Li	IRC Standards Review Committee and Security Working Group		X								
		Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
		1. James Castle	NYISO	NPCC	2								
		2. Bill Phillips	MISO	MRO	2								
		3. Mark Thompson	AESO	WECC	2								
		4. Patrick Brown	PJM	RFC	2								
		5. Matt Goldberg	ISO-NE	NPCC	2								
		6. Steve Myers	ERCOT	ERCOT	2								
		7. Lourdes Estrada-Salinero	CAISO	WECC	2								
		8. Charles Yeung	SPP	SPP	2								

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		9. Dave Dunn	IESO	NPCC		2							
		10. Tobias Hendricks	MISO	MRO		2							
		11. Kelly Ryan	MISO	MRO		2							
		12. Elliot Gordon	NYISO	NPCC		2							
		13. Brett Lewis	NYISO	NPCC		2							
		14. Gregory Goodrich	NYISO	NPCC		2							
		15. John McGlynn	PJM	RFC		2							
		16. Steve McElwee	ERCOT	ERCOT		2							
		17. Jim Brenton	ERCOT	ERCOT		2							
		18. Ann Delenela	ERCOT	ERCOT		2							
		19. Garry Spicer	SPP	SPP		2							
		20. Philip Propes	SPP	SPP		2							
		21. Ryan McCon	SPP	SPP		2							
		22. Tim Lockwood	CAISO	WECC		2							
		23. Jamey Sample	TVA	SERC		2							
		24. Joe Pereira	ISO-NE	FRCC		2							
106.	Group	Richard Kafka	Pepco Holdings, Inc.	X		X		X	X				
		Additional Member	**Additional Organization**	**Region**		**Segment Selection**							
		1. Richard Kafka	Potomac Electric Power Company	RFC		1							
		2. Mark Godfrey	Delmarva Power & Light	RFC		1							
		3. Timothy Hadfield	Delmarva Power & Light	RFC		1							
107.	Group?	Bill Gross	NEI										

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

Summary Consideration:

Response:

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Progress Energy	Disagree	Change to read: "A discrete set of one or more routable or dial-up programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data."
GSOC/OPC	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn't in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define "systems" as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word "organized" should be changed to "configured".
Hayden	Agree	1. Consider inclusion of "testing" in the list of functions. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? As I think through the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. Suggest you specifically address this and any other quesitons from FAQ for CIP-002 in the standard.
SDGE	Disagree	We feel that this is an overly broad definition for relevant cyber systems. We suggest rewording the Cyber System definition as follows: A discrete set of one or more programmable devices organized for the collection, storage, processing, maintenance, and communication of data". Under the proposed definition of Cyber System, certain non-relevant items could be in-scope that are unnecessary. We think it is more prudent to limit the scope and potentially eliminate unnecessary confusion.
APPA	Agree	However, see below the discussion of BES Cyber Systems.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Consumers	Disagree	There is no need to introduce this term. See Section 13. This definition seems to include all electronic components within a substation, many of which either have no control capability or cannot independently control elements of the BES. eg, a simple electronic panel meter with no outside (the ESP) connectivity would be included. We'd suggest the following wording: "A discrete set of one or more programmable electronic devices capable of controlling elements of the BES and which is/are accessible remotely. We would go on to further define "access remotely" with the same criteria used in CIP-002-3, R3, of "… uses a routable protocol" or "is dial-up accessible". In addition, this definition, and other NERC guidance documents seem to imply that entire SCADA systems, Remote Relay Setting (or file acquisition) Systems, etc, would be included, even though only the portion located at the Control Center would be accessible via any commonly know threats utilizing dial-up or routable protocols. This change in terms would then include individual RTUs, relays, fault recorders, regardless of the fact these present an almost non-existent risk of being hacked. Although we respect the intent of trying to cover "systems" the definition cannot be so broad to thereby include every piece of every system, regardless of its unessential BES reliability contribution or the lack of accessibility to it remotely. NERC should refrain from using the word "risk". As a caller pointed out there is confusion as to whether impact or probability is the intended meaning. Specifically, in the definition of High BES Impact, take out the words "an unacceptable risk" after the word create in both instances it is used in the definition. "An unacceptable risk" also appears in the definition of Low BES Impact, it should be removed from there also.
NPCC	Agree	
SWPA	Disagree	With inclusion of BES Cyber System definition with proposed changes (below), this definition is not needed. This definition should be deleted and BES Cyber System definition changed as written in comment for 1.b.
MPPA	Agree	
Central Lincoln	Disagree	Since all cyber components are generally interconnected, it is unclear where one system ends and another begins. Any set chosen will have connections to other sets, and therefore not be a discrete set. Discrete: adj. Consisting of unconnected distinct parts.
Dominion	Disagree	Dominion proposes the definition be modified to state: "Cyber System — A discrete set of one or more Cyber Assets that communicate via routable protocol." As currently defined, the term would apply to all programmable electronic devices and expand the scope of applicability without providing additional reliability to the Bulk Electric System. The modified definition clarifies the intent of the term by limiting the scope of applicability to programmable electronic devices and communication networks (including hardware, software, and data), all of which have the potential to adversely affect the Bulk Electric System.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Encari	Disagree	Requirement R3.1 implies that any Cyber System within a BES Subsystem that is identified under the criteria in Attachment 1 has the potential to be a BES Cyber System. That may not be the case since the definition of a Cyber System is not tied or related to the definition of a BES Subsystem. In order to ensure the implied relationship exists, we recommend the definition of BES Cyber System be expanded to state, "A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. A Cyber System associated with a BES Subsystem identified under the criteria in Attachment 1 is presumed to be a BES Cyber System if the Cyber System has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System."
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the proposed definition is overly broad and may include systems unrelated to the Bulk Electric System. Therefore, SCE proposes that the definition be more narrowly defined by adding the phrase "which support functions essential to the bulk electric system" to the end of the proposed definition.
USBR	Agree	
Dyonyx	Disagree	We believe there needs to be some clarification of the issue of "Communications equipment" being included or excluded as a BES Cyber System. Will an Entity that owns their "communication equipment (e.g., microwave system)" be required to classify and then apply security controls while an Entity that does not own its "communications equipment" (i.e., uses TELCO T1s, etc.) not be required to apply controls?
FMPP	Agree	
Westar	Agree	
Green Country	Agree	
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Wolverine	Agree	
Portland GE	Disagree	PGE does not agree with this definition for several reasons, including the fact that it does not specify something that "communicates," which is the risk these standards are attempting to address. Rather, it uses the even more ambiguous term "programmable;" this word must be defined. In addition, the word "critical" is being eliminated so that all systems are identified and ranked. That would imply that CIP is also an outdated term and may change to SIP or System

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Infrastructure Protection. The concept of ranking all grid facilities seems ambitious, and PGE questions whether the benefits of such a broadly scoped endeavor would justify the costs.
PSEG	Disagree	Comment #1: There are a number of new terms introduced. We would like a description of how the terms interrelate with each others and how the related to the previous version terms used such as “Cyber Asset” and “Critical Cyber Asset”. • More formalism is required to define what elements can constitute or be part of each term. For example, are Generation Subsystems a type of BES Subsystem or a constituent of a yet undetermined BES Subsystem? • Is a particular BES Cyber System to be treated as a single “atomic” entity or is a BES Cyber System composed of cyber assets that need to be investigated separately. • What is the definition of the word “element” used in the definitions of Generation Subsystem and Transmission Subsystem? Should the phase shared “shared Cyber System” be replaced with “shared BES Cyber System”? • The definition of what constitutes a Generation Subsystem or Transmission subsystem is whether these categorizations of assets “… become unavailable due to loss or compromise of a shared element of a shared cyber system”. How can this italicized statement be known a prior? Categorization is BES Subsystem is an R1 requirement that is not dependent on knowledge of whether a “cyber asset” can be compromised. Comment #2: What does the group mean by a programmable electronic device for “maintenance”, “communication” and “use”? (Could the SDT please provide an example of each type of device?) Comment #3: Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? Comment #4: We believe that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be program over the internet or through a routable device.) EEI’s proposed definition for Cyber Systems: “Cyber System – a discrete set of one or more programmable electronic devices organized in a collection , storage ,processing , maintenance , use , sharing, communication, disposition or display of data WHICH SUPPORTS FUNCTIONS ESSENTIAL TO THE BES ..” seems to better define the term. Comment #5: We believe that the monitor’s which only display data should not be included as part of a Cyber System. Our understanding: We understand the term, “Cyber System” to imply one or more electronic device(s) that are part of an interconnected (networked) within an Electronic Security Perimeter (ESP) with the capability to be programmed remotely (offsite). Comment #6: We are concerned about the inclusion of maintenance, sharing, communication, disposition, and display. Comment #7: There is no need to introduce this term. Suggestion: “Has the capability to remotely acquire and modify real-time BES system data, send control signals to, or modify the

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		settings of a programmable electronic device(s).” Our suggestion addresses either “open” (e.g. internet), “closed” (e.g. private fiber optic network) or a combination of the two different network configurations. Entities must be allowed the ability to factor in their network configuration as part of the engineering analysis
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. The current definition is too broad and implies the inclusion of electronic devices that would not have anything to do with the BES. The definition of Cyber System does not include the category of control. We further recommend more clarity in the list of attributes. For example, does "maintenance" apply to test equipment, data, etc.? A cyber system has traditionally been identified as one that uses a routable protocol and therefore can be network connected.
Idaho Power	Disagree	Programmable electronic devices could be interpreted to exclude certain types of cyber assets. Replace with cyber assets instead.
SOCO	Disagree	This definition will force inclusion of all electronic components within a substation, many of which either have no control capability or cannot independently control elements of the BES. Suggest the following wording: “A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data and has the ability to independently control elements of the BES.” The term as defined would include most if not all instrumentation equipment installed within a Generation Unit. Even a simple stand alone 4-20 mA control loop consisting of a typical pressure transmitter, control panel mounted analog controller and a control valve, with no connection possibility to any “network”, would be included in the defined scope of a “Cyber System”. Within the described loop any of three components would trigger inclusion. All of these devices are programmable from the standpoint that their calibration parameters may be adjusted and the related setting stored to local onboard memory. Care should also be taken in the wording to avoid inclusion of terms, which could include technology such as HART protocol, which allows configuration based on physical access to the device or connection to the analog signal control wiring at the same geographic location. As presently written this definition would include even temporary performance monitoring and testing systems which are used for data acquisition and performance enhancement and which in no way connect to control and command systems or have a potential to impact the operation of a generation unit. This definition should address only those upper level systems, which are capable of being electronically accessed and manipulated from an offsite location. Suggested definitions are: Cyber System – A set of one or more “remotely accessible” programmable electronic devices organized for the collection, storage processing maintenance use sharing, communication, disposition or display of data.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
DTE	Disagree	This definition needs revision to remove devices that do not use routable protocols from the scope of the standard. Similarly communication networks between discrete ESPs should not be in scope.
AEP	Disagree	AEP appreciates the extensive efforts of the SDT in the preparation of the version 4 draft standard. The SDT may well be trying to provide registered entities with greater flexibility in defining its applicable assets and systems, but the open-ended nature of this definition and of the standard in general, is of concern. Ultimately, the audit teams will determine if the registered entity included the assets and systems that it should it should have and, to this end, most entities would prefer to have “bright lines” that clearly state what is in scope and out of scope. Without some limitations, all programmable devices may be considered cyber assets, including those not connected to a network could be included as in scope under the provided definition. For example, all generator and transformer digital protective relays could be considered in scope even if its not network connected. Risk levels will differ based on the type of interface, connection, and controls. The standard language is even blurring the line between computers and control system equipment. Alternatively, we would suggest adopting the Control System definition from NIST SP800-82 and striking the Cyber System definition. NIST SP800-82 makes it abundantly clear that industrial control systems are different than traditional IT systems. Consistent with FERC’s Order, it would be helpful to the team to leverage this NIST work as it highlights the work industries and government organizations are to advance control system security. Accordingly, the suggested Control System definition would be: An information system used to control processes such as manufacturing, product handling, production, and distribution. These systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Disagree	N&ST believes, based on experience with the current Standards, that definitions intended to allow for flexibility and to "cast a wide net" tend to lead to endless, and often unproductive, debate over their precise meaning. At a minimum, we recommend that the SDT consider addressing both the logical and *physical* proximity of a "cyber system's" components in order to forestall arguments over whether or not a "cyber system" can span multiple locations (e.g., a set of field assets, such as RTUs, feeding data to a control center at another location).
Flathead	Disagree	I do not think constantly creating new definitions without clarifying existing definitions and acronyms is efficient. I believe the existing definitions should be retained or modified. Also the Bulk Electric System vs. the Bulk Power System, the most key definition of all is still not properly clarified by the regions. Shouldn't that be the focus before creating new subsystems that may include both BES and non-BES assets. This definition has the potential of diverting resources to non-critical non-BES assets that are truly "low impact" and should not be part of this evaluation, defeating the purpose of protecting critical assets.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
E ON	Disagree	The definition would include standalone devices, i.e., non-networked devices, that perform any one of the listed functions. Keeping in mind the purpose of preventing unauthorized access, the definition is far too inclusive. A stand-alone programmable logic controller cannot be accessed except by an individual in the plant with proper MMI. An on premises individual could disable plant operations far more easily by simply operating switches on the control panel.
Carthage	Agree	
WECC	Agree	The word programmable might lead to confusion in the future as entities may be unsure if it refers to programmable by them or the manufacture or both. The word doesn't seem necessary in the definition.
Entergy	Disagree	Anything with EPROM would seem to apply, though may not necessarily be relevant.
CenterPoint	Disagree	CenterPoint Energy does not support the direction the SDT is taking with the introduction of multiple new definitions. One of the four key principles driving the SDT's work is to "build on work already done to comply with Version 1 of the CIP reliability standards, including the industry's experience and investments." The proposed changes do not align with that principle and in fact appear to start over with new concepts. Considering the considerable effort that registered entities have already expended to comply with the existing standards under the existing categorization of assets, it does not make sense to "reinvent the wheel" at this juncture. Furthermore, the proposed new set of definitions in CIP-002 would be incompatible with CIP-003 through CIP-009. CenterPoint Energy understands the SDT's intent would be to conform CIP-003 through CIP-009 over time in some piecemeal fashion to the new paradigm introduced in this version of CIP-002. CenterPoint Energy believes the SDT's piecemeal implementation plan is unrealistic and will add even further confusion to the CIP standards. Indeed, much of the CIP-003 through CIP-009 requirements would not make sense for anything other than Critical Assets, roughly equivalent to the proposed "High BES Impact" paradigm introduced in this draft. A specific concern with the proposed definition of cyber system is the inclusion of "communication" as one of the possible attributes that define a cyber system. The considerable vetting by the industry over the many years produced the appropriate conclusion that communication devices are outside the definition of BES cyber assets. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are exempt from the existing Standard CIP-002 in section 4.2.2. This exemption should remain in version 4 because these common carrier communication lines are often leased from third party telecommunication companies who should be responsible for the protection. CenterPoint Energy believes the SDT may have intended to capture the concept from the existing CIP-002 version that an electronic device must communicate by routable or dial-up communication mediums in order for the device to be considered a cyber asset. However, as written, one could misinterpret the definition as meaning that communication mediums themselves are cyber assets, which would not be appropriate. The definition of a cyber system should be reworded as follows: Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage,

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		processing, maintenance, use, sharing, communication, disposition, or display of data, which communicates externally through a routable or dial-up communication protocol.
CA Cogen	Agree	
LCRA	Agree	
FRCC	Disagree	The Definitions proposed by the SDT for Bulk Electric System Subsystem states, “A group of one or more BES Facilities…”. Per the NERC Glossary of Terms a Facility is a set of electrical equipment that operates as a single BES Element. Therefore a subsystem is a group of elements and if you replace ‘subsystem’ with ‘element’ in the requirements the intent of the requirement remains intact and you are not introducing confusion by redefining a portion of the BES (i.e. BES Subsystem, Transmission Subsystem and Generation Subsystem). If additional clarity is desired by the SDT, a revision to the current definitions of Element, Facility and Transmission should be considered before new terms are introduced to the industry.
NIPSCO	Disagree	We are concerned about the inclusion of the terms maintenance, sharing, communication, disposition, and display. Suggestion: Further clarifications on the intent of this language as well as examples of device types are needed.
ConEd	Disagree	Real-time Operations: There should be a requirement that the system is used for real-time operation and/or to make real-time decisions. Interconnectedness: There should also be a requirement that the Cyber System is networked or connected somehow outside the station. The definition should include that the fiber system has connectivity to the outside environment such that it can be hacked. Cyber system assets are too broadly defined and the definition does not taking into account that the systems in many cases are protected by physical isolation, locked cabinets and/or rooms.
EEI	Disagree	EEI believes that this definition is overbroad and potentially brings in an inappropriate number of devices that should not be in scope for the standard, e.g. display terminals, personal cell phones, pagers etc. The definition of Cyber System includes “communication.” This phrase should either be defined more precisely or removed. The definition of Cyber System includes “disposition.” This phrase should either be defined more precisely or removed. EEI suggests the following revision: Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access, that support functions essential to the bulk electric system.
O&R	Disagree	Real-time Operations:

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		There should be a requirement that the system is used for real-time operation and/or to make real-time decisions. Interconnectedness: There should also be a requirement that the Cyber System is networked or connected somehow outside the station. The definition should include that the fiber system has connectivity to the outside environment such that it can be hacked. Cyber system assets are too broadly defined and the definition does not taking into account that the systems in many cases are protected by physical isolation, locked cabinets and/or rooms.
Alliant	Agree	
Ameren	Disagree	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. Also, if “communication” devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of Cyber System includes “disposition.” This phrase should either be defined more precisely or removed. Add to the end of this definition “that together perform a specified function”.
Black Hills	Agree	The definition itself is technically sound, but it implication is profound because virtually all programmable electronic devices would be included by the definition.
TNMP	Disagree	TNMP believes the current Cyber System definition fails to establish clear criteria or “bright lines” the drafting team is attempting to put into the standards. The definition fails to clearly convey how the discrete sets of devices are grouped together into a Cyber System. Some statement binding the devices based upon function or mission objective would help. However, the reason for a revision of CIP-002 is to eliminate the Responsible Entity from being tasked with developing a risk methodology and to create a uniform methodology across the industry. The proposed standard shifts the problem of defining Critical Cyber Assets to defining Cyber Systems without appreciably addressing industry uniformity. The definition needs to be greatly improved since it is the basis definition for BES Cyber System to which future CIP-003 through CIP-009 standards apply. A few examples of how the current definition lacks clarity: Is a SCADA System restricted to Master servers and operation workstations? Are the RTUs which reside in many BES Subsystems included in the proposed definition? Does RTU communication system architecture (e.g. centralized modem bank, distributed banks with Ethernet conversion, direct Ethernet) contribute to determination if the RTUs are Cyber Systems? Are RTUs and their communication systems to be considered part of the SCADA Cyber System? Can isolation of communication systems via network firewalls exclude devices such as RTUs from inclusion in a SCADA system?

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Should the RTUs be considered part of the SCADA Cyber System given that the ability to manipulate the RTU in a manner that would result in successful manipulation of the main SCADA Cyber System is extremely limited and unlikely? Other examples of lack of clarity arise in the application of the definition to the relay systems in a substation: Would a Relaying Cyber System be comprised only of devices within a single substation or all relaying across any connected substations? Would the Relaying Cyber System be grouped by the relays interaction with other relaying? This possibility could result in several relay systems along a transmission path being considered a singular Relay Cyber System. In summary TNMP believes the current definition lacks clarity to help the industry implement meaningful cyber security measures, and makes it difficult for NERC to properly audit Responsible Entities uniformly.
NVEnergy	Disagree	The use of the qualifier “one or more” leaves open the question of what discretion is allowed the Entity to group these devices together. We believe this will lead to confusion or inconsistency in application. We suggest to the Standards Drafting Team that this definition be restricted to the discrete cyber device level, rather than allowing discretion as to the number of cyber devices that should be collected to form a “system” Also, the very word “Cyber” should require that the system is accessible via remote locations from the device.
MWDSC	Disagree	Too vague a definition which could apply to any electronic device within a local facility. Needs to include some form of communication device, e.g., RTU or modem, which interfaces with a control center. For example, some protection devices in substations automatically react to power flows and do not require a control signal from a remote location. Recommend adding a phrase at the end such as "..,or display of data, and communicated to a Control Center at a remote location."
Empire	Disagree	Option for consideration for definition of Cyber System: Programmable electronic devices and communication networks including hardware software and data.
NCEMCS	Disagree	I Agree in concept, however this definition includes all electronic devices of which many will have no control capability or cannot independently control elements of the BES
BCTC	Disagree	See Question 13
SWTC	Disagree	SWTC has some concerns with this new standard, as it all based on BES Assets, and their impact. I am under the assumption that the Bulk Electric System Task Force is trying to rewrite the BES Definition. It appears that until the BES is defined, then any assumptions presented in CIP-002-4 are under the old definition, which is almost like putting the cart before the horse.
SCEG	Disagree	While the majority of cyber systems may be organized for the data purposes described, others only use data as a tool for another purpose. For instance, a physical access control cyber system is not organized for the collection, etc. of data. The data is simply a means to an end. It is organized for access control. The definition could be improved by avoiding the concept of what the system is for entirely. Suggested wording: "A discrete set of one or more programmable electronic

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		devices that collects, stores, processes, maintains, uses, shares, communicates, disposes of, or displays data." We also feel that "Test and Validation" and "Recovery" should be added to the definition.
Exelon	Disagree	Exelon has concerns with the proposed CIP standard definitions that may result in overlaps and/or conflicts in definitions between the regulatory entities (NRC, CNSC, and NERC). We ask that NERC and/or the SDT take action to ensure the proposed definitions are reviewed and revised if needed to eliminate any potential overlaps. Exelon also has concerns with the ambiguity introduced into the definition by including “communication” and “disposition”. We suggest the following as the definition: Cyber System – A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing or display of data which support functions critical to the Reliable Operation of the Bulk Electric System (i.e. Attachment 2)
BPA Trans	Disagree	This definition is better than the one for Cyber Assets but still leaves some unanswered questions regarding exactly what would qualify as a Cyber System. The term “programmable electronic device” must be defined. The following definition is suggested: "capable of executing code installed into volatile memory by end users". If not defined, then the use of the word “programmable” is problematic. Many industrial control devices, which may use microprocessors, can have their settings changed and could be considered “configurable,” but users cannot “program” them in the classic IT sense of the term. The base functions of onboard software cannot be changed nor can new software be written, compiled, or installed on them except by the vendor. Question 1: Is it intended that the terms “set,” “configure,” or “program” are meant to be interchangeable with “programmable?” Question 2: Is a device that has a limited specific set of factory defined capabilities considered “programmable?” Some examples of installed equipment that need a determination of “programmable” are: • A device that is limited to being “set” or “configured” through a vendor provided user interface, within device limitations, or • A device not capable of having its base programming altered while in operation, or • A device that requires specific vendor supplied hardware to change or update, or • A device that must be flashed or have EPROMs replaced for updates, using vendor provided interface/ports and with vendor provided updates, or • A device not capable of having additional applications installed, or • A device that has no onboard memory locations that can hold extraneous programs. Question 3: What about non-cyber “Cyber Systems,” such as: • Devices that operate on a microprocessor platform and could be defined as Cyber Systems even though they have no other attributes of a Cyber System? These devices, while possibly providing support to the BES

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Subsystem, present no potential for vulnerability or degradation of the BES, or • Devices that only provide interface for viewing information, but cannot be controlled, nor does it provide control, or • Devices that are microprocessor based but have no communications connections, or • Devices that are microprocessor based which may be directly affected only physically at the device. • If the connection between two devices is a simple electrical on/off connection (firing of alarm points) does it constitute a Cyber System? • Is a microprocessor based relay (supports the operation of a BES Subsystem) but is not connected to any form of communications so must be assessed manually and operates autonomously, a "Cyber System?" The new definition of "Cyber System" is all-inclusive. It appears that the SDT intends to capture any and all electronic devices under the umbrella of this definition: Table of Purpose Elements and potentially included Devices/Systems: Purpose Element Devices/Systems that may be included Collection (of data*) Relays, DFRs, SER, TTrip, PMU, RAS RTU, Controller and IDP Laptops, Others? Storage (of data*) Relays, DFRs, SER, TTrip, PMU, RAS RTU, Others? Processing (of data*) Relays, TTrip Controller and IDP Laptops, Others? Maintenance(of data*) Not sure how to address this one. Devices don't generally maintain data, people do. Use (of data*) Relays, Firewalls, Laptops, Others? Sharing (of data*) Interfaces on Firewalls, Relays, D400s, Others? Communication (of data*) Networks and other communications infrastructures? This is significant as it may draw in The FIN, SONET, DATS, Microwave Radio System, Modem Connections and other communications equipment. Disposition (of data*), or This may be the archiving or destruction of data. We are not sure. display (of data*) Web interfaces, Laptops, simple HMI interfaces, SEMM, RAS, Alarm Systems. What would be included? * - The focus is on "data," which is typical for security of IT systems. The argument can be easily made that nearly all electronic devices perform one or more of these functions. Is this what the SDT intended? The rest of the definition is almost straight out of the National Institute of Technology (NIST) Interagency Report 7298 (NISTIR-7298). We believe that this is good.
HQT	Agree	

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Allegheny Supply	Agree	
KCPL	Disagree	No, this is too broad in regards to “of data”. The CIP Standards should limit themselves to the equipment and data used only for the monitoring and control of the BES.
Connectiv Energy	Agree	
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13. This definition is not needed at this time. If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time. Further, there is value in retaining the existing definitions of Critical Cyber Asset and Cyber Asset (but clarifying what is meant by “network”) and the qualifying characteristics of routable protocol or dial-up. Security controls will still be applied to distinct, discreet, individual Cyber Assets, not generically defined “systems.” If categorization proves the value and need for defining the term Cyber System, the definition should be “a group of Cyber Assets that communicate by routable protocol and/or are dial-up accessible.” This solves the problem with the draft definition in CIP-002-4 of being overly broad and bringing in a number of devices that should not be in scope because they are not vulnerable to a concerted, well-planned attack against multiple points; including, for example: display terminals, cell phones, pagers, as well as many kinds of devices that cannot be accessed or manipulated from a remote location.
CPG	Disagree	This definition of cyber system is extremely broad and encompasses too many items. What is lost in this definition is that these systems may not be critical to the operation or protection of the BES element, and would therefore not be critical to the BES. To have entities list every cyber system does not have an impact on the safety and reliability of the BES. This term should be combined into the BES Cyber System terminology.
Santee Cooper	Agree	Santee Cooper Introductory Comments: As a whole, Santee Cooper (SC) supports the general framework of the new version. However with this new version comes an enormous amount of procedural and policy overhauls. SC would support a phased-in approach as opposed to a deadline for compliance. In addition SC would not want to vote on this standard alone. Because new versions of CIP-003 through CIP-009 would also be required, and those would define the different levels of requirements for the impact levels, SC would rather vote on CIP—02 through CIP-009 as a total package.
OGE	Disagree	• Provide a description for the term "disposition". What is your intent for including this term. • Provide a definition/description for the term "Communication" How does section "4. Applicability: 4.2.2. "Cyber assets associated with communication networks ….” found in Standards CIP 002-1, CIP 002-2 and CIP 002-3. There is an exemption for cyber assets associated with communications between ESPs. Will this exemption carry to the version 4 standard?

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		• Is there any processor based device that does not fit this definition?
Oncor	Disagree	There is no clarity as to what makes up a “cyber system”. Is my SCADA system a Cyber System? Is a single programmable relay at a substation a cyber system or do all the relays at a substation makeup a single cyber system?
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Disagree	1. Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? National Grid believes that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be programmed over the internet or through a routable device.) 2. Please provide example of programmable electronic device organized for “maintenance”, “use”, and “communication” 3. Monitors which only display data should not be part of Cyber System
MGE	Disagree	MGE understands why the SDT is defining Cyber System, establishing a basis for “BES Cyber System” but the proposed definition must clarify that it applies to Cyber Systems that support the reliable operation of the BES where as to maintain equipment and electric system’s thermo, voltage and stability limits so that instability, uncontrolled separation, or cascading failures do not occur, as written in question 1.g. As written, every computer, cell phone, or storage device (ie, thumb drive) would be considered a Cyber System no matter if it is for BES operations or personal use. Please clarify what “maintenance, communication and use” means in the proposed definition. The displaying of data (a monitor) should not be included. The displaying of data is received from a CPU or SCADA system, the monitor has no impact or ability to perform an action that would disrupt the BES. Recommend that the definition apply to devices that are electronically accessible. An electromechanical relay can be programmed but not via the internet or through a routable device.
FE	Disagree	The definition should be limited to programmable electronic devices that have the ability to be accessed remotely and pose risks to a coordinated attack. The definition is open-ended and could easily be misinterpreted and inadvertently include devices that would pose no risk to the BES; cell phones, pagers, computer terminals, etc. FirstEnergy offers a slightly modified version of the definition offered by EEI. We have removed the phrase "that support functions essential to the bulk electric system" from the EEI version as the BES Cyber System definition brings in that aspect. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
TECO	Disagree	Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data that supports functions essential to the bulk electric system.
CECD	Disagree	CECD supports having a separate definition for Cyber System. The definition should explicitly exclude analog devices and the communication networks and data communication links between discrete Cyber Systems. In addition, as indicated in our discussion on the definition of BES Subsystems, we do not feel it is appropriate to include a control center in that definition, but instead would prefer that the control center be defined as a Cyber System to be evaluated for its impact on/interaction with BES Subsystems to determine if the control center qualifies as a BES Cyber System.
MRO	Agree	The MRO NSRS approached every question as if it were in a vacuum, attempting to answer the individual questions honestly without being persuaded by the remainder of the standard. This meant addressing the questions as written and including comments only in the appropriate areas. While we may agree with the individual questions being asked, we request that the SDT give particular consideration to our comments found in question 13, which details our thoughts on the overall approach of the CIP-002-4 draft standard.
GTC	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn't in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define "systems" as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word "organized" should be changed to "configured".
Xcel	Agree	
BGE	Disagree	We believe that the definition of "Cyber System" is unnecessary and that item 1.a. should be deleted. The standard should only deal with BES Cyber Systems and this definition of Cyber System can be rolled into BES Cyber Systems.
Springfield, MO	Agree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		TAPS supports the comments submitted by the MRO NSRS regarding this project, as well as the modifications to the standard proposed by APPA. TAPS submits these separate comments to object to the proposed three-tier approach, and urge the inclusion of a fourth, "No Impact" tier. Specifically, TAPS emphasizes its concerns with respect to the treatment of "Low BES Impact" subsystems and cyber systems, set out in response to Questions 1(i), 2, and 8, below. As this proposed standard appears to be largely implementing the Categorizing Cyber Systems Concept Paper issued by NERC in July 2009, please see as well TAPS' comments on the Concept Paper, submitted September 4, 2009.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Allegheny power	Disagree	AP believes that this definition is overbroad and potentially brings in an inappropriate number of devices that should not be in scope for the standard, e.g. display terminals, personal cell phones, pagers etc. The definition of Cyber System includes “communication.” This phrase should either be defined more precisely or removed. The definition of Cyber System includes “disposition.” This phrase should either be defined more precisely or removed.
FMPA	Disagree	Intro: First, let FMPA congratulate the CIP Standard Drafting Team for creating a good framework for identifying the focus of what is to be regulated concerning cyber security and focusing that regulation on what is important to ensuring BES reliability. Although FMPA has checked the “disagree” box on many of these questions, we believe the general framework to be sound and most of FMPA’s comments are geared towards reducing the complexity of the standard, to help clear up ambiguity and reduce subjectivity, to contribute to the technical expertise discussions, and to increase the clarity of the standard. With those foci in mind, we offer the following comments which we hope you find constructive. Comments: One would assume that a Supervisory Control and Data Acquisition (SCADA) would be a Cyber System, yet there is no mention of “Control”, which would seem to be the characteristic of a Cyber System with the highest impact to BES reliability.
Duke	Disagree	This definition should be revised to exclude field wired devices that happen to be programmable. Suggested wording: Cyber System – A discrete set of programmable electronic devices connected together via an active communications protocol.
AESI	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn’t in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define “systems” as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word “organized” should be changed to “configured”.
IESO	Agree	
Manitoba 2	Disagree	Please clarify the meaning of the word “maintenance” as it applies in this definition. Please clarify the meaning of the word “disposition” as it applies in this definition. If the intent is to mean “the way in which something is arranged”, that is included under display of data. If the intent is to mean “the transfer of property to someone”, that is included under sharing of data. The Cyber System definition needs to be clearer regarding the determination of the boundaries of a cyber system. Please define “programmable”. Is every electronic device which is configurable by any means (switches, dials, settings)

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		considered a "programmable" device? Should an electronic device, such as a protocol converter which is settable, be considered a cyber system, or is it really meant to focus on intelligent electronic devices and systems? Security requirements also need to consider the capabilities of the devices. Are cyber systems which primarily support a maintenance activity related to a BES Subsystem to be included in the scope of this definition? If, so how is it limited to the most important activities? Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Agree	
ATC	Disagree	Concerns with the proposed definition: 1. What does the group mean by a programmable electronic device for "maintenance", "communication" and "use"? (Could the SDT please provide an example of each type of device?) 2. Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? 2.1. ATC believes that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be programmed over the internet or through a routable device.) 3. ATC believes that the monitor's which only display data should not be included as part of a Cyber System. Our understanding: We understand the term, "Cyber System" to imply one or more electronic device(s) that are part of an interconnected (networked) within an Electronic Security Perimeter (ESP) with the capability to be programmed remotely (offsite). Suggestion: "Acquires / collects real-time BES system data, sends control signals to BES Facilities either through command functions or settings and is programmable by remote access." Our proposed definition is attempting to identify only those electronic devices that control an action or collect real-time data on the BES. We believe that this standard should not identify such devices as firewalls, switches or routers. This separation provides the SDT the ability to develop different controls around the distinct groups of devices and should result in the elimination of a number of current TFE requests. In addition, our suggestion addresses either "open" (e.g. internet), "closed" (e.g. private fiber optic network) or a combination of the two different network configurations. Entities must be allowed the ability to factor in their network configuration as part of the engineering analysis.
LES	Disagree	We support the MRO NSRS comments with the following additional items: If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).
PSE	Disagree	Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access. Puget Sound Energy supports the inclusion of all definitions in the NERC Glossary with used consistently across all standards versus localized definitions that differ across different applications.
IMPA	Disagree	IMPA proposes the following definition for Cyber System. Cyber System - A discrete set of one or more programmable electronic devices grouped together to perform the following functions: the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data as required by Control Centers, Generation Subsystems, and/or Transmission Subsystems for the reliable operation of the Bulk Electric System.
ERCOT	Disagree	The current definition lends itself to misinterpretation and expansion of the intent. Recommend that the definition clarify that a Cyber System as a discrete system where all components contained within act as common functional elements of the system and individual components, whether or not they are capable of being programmed, are not considered separate Cyber Systems. Request that the drafting team provide clarification regarding categorization and classification of cross platform infrastructure systems. This should include guidance on components that are exchangeable or hot swappable without any impact on the Cyber Systems utilizing that component.
PacifiCorp	Disagree	See PacifiCorp's summary comments in question 13. This definition is not needed at this time. If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time. Further, there is value in retaining the existing definitions of Critical Cyber Asset and Cyber Asset (but clarifying what is meant by "network") and the qualifying characteristics of routable protocol or dial-up. Security controls will still be applied to distinct, discreet, individual Cyber Assets, not generically defined "systems." If categorization proves the value and need for defining the term Cyber System, the definition should be "a group of Cyber Assets that communicate by routable protocol and/or are dial-up accessible." This solves the problem with the draft definition in CIP-002-4 of being overly broad and bringing in a number of devices that should not be in scope because they are not vulnerable to a concerted, well-planned attack against multiple points; including, for example: display terminals, cell phones, pagers, as well as many kinds of devices which cannot be

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		accessed or manipulated from a remote location. .
PEPCO	Disagree	Parts of the Cyber System definition are too broad and overreaching with the potential of including unintended devices that do not necessarily need to be in-scope. Not all programmable devices are able to be reprogrammed or have the storage capacity to have an Operating System. The definition as presently written could include coffee makers, televisions, radios, mp3 players, DVDs, PC projectors, telephones, watches/clocks, USB storage devices, thermostats, thermometers, navigation systems, pagers, barcode scanner, and/or 2-way radios. The definition seems to focus on data (e.g. storage, maintenance, use, sharing, displaying) and not necessarily on cyber control systems which should be the main focus. The current definition could lead to confusion. Clarity and more precise definitions are needed for terms such as – a discrete set of one, programmable electronic devices, communication, and disposition of data. . We suggest the following: Cyber System - Suggest that the define term of Cyber System not be used. Rather start off with the BES Cyber System definition. If the SDT feels that this term is still needed, suggest that examples of “Cyber System” devices be provided for each item included in the definition (e.g. collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data) to provide clarification.
NEI	Disagree	A) It does not describe the functions, and the use of “data” is vague and needs better definition. B) There is no language about routable protocols – need to add “that communicate via a routable protocol.” C) NEI recommends “A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access.” D) The SDT may well be trying to provide registered entities with greater flexibility in defining its applicable assets and systems, but the open-ended nature of this definition and of the standard in general, is of concern. Ultimately, the audit teams will determine if the registered entity included the assets and systems that it should have and, to this end, most entities would prefer to have “bright lines” that clearly state what is in scope and out of scope. Without some limitations, all programmable devices may be considered cyber assets, including those not connected to a network could be included as in scope under the provided definition. For example, all generator and transformer digital protective relays could be considered in scope even if it is not network connected. Risk levels will differ based on the type of interface, connection, and controls. The standard language is even blurring the line between computers and control system equipment. E) Alternatively, we would suggest adopting the Control System definition from NIST SP800-82 and striking the Cyber System definition. NIST SP800-82 makes it abundantly clear that industrial control systems are different than traditional IT systems. Consistent with FERC’s Order, it would be helpful to the team to leverage this NIST work as it highlights the work industries and government organizations are doing to advance control system security.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Accordingly, the suggested Control System definition would be: An information system used to control processes such as manufacturing, product handling, production, and distribution. These systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Summary Consideration:

Organization	Yes or No	Question 1.b. Comment (Response page 6)
Progress Energy	Disagree	Add the following to the end of the definition: "as defined in CIP-002-4 Attachment 1."
Dynegy	Disagree	Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems "also includes all of the components necessary to ensure the protection of the reliability function(s) being performed". If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
GSOC/OPC	Disagree	If "functions critical to the reliable operation of the Bulk Electric System" is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2. The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
Hayden	Agree	
SDGE	Disagree	"Critical" and "adversely" need to be defined or have examples provided. Even the phrase "has the potential" lends additional vagueness to the definition. We are advocating a simpler approach to make the definition easier to understand and apply. We propose the following wording: A Cyber System, which if rendered unavailable, degraded, or compromised, would impact the reliable operation of the BES.
APPA	Disagree	APPA Task Force Prefatory Comments: The APPA CIP Task Force supports the general framework for BES cyber-security proposed by the CS706 Standards Drafting Team ("the SDT") and commends the team for its work. While we have checked "Disagree" for many of comment boxes below, in each case we have attempted to provide constructive comments to improve upon the clarity and quality of the draft standard and where possible, to simplify the steps that registered entities must undertake to ensure both BES cyber-security and auditable compliance. Should you have any questions concerning these comments, please do not hesitate to contact us. We look forward to reviewing and commenting upon the next draft of CIP-002-4, as well as the associated security controls being developed under CIP-003-4 through CIP009-4.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		APPA Task Force Suggested Definition: BES Cyber System - A discrete set of one or more programmable electronic devices that are organized to control generation or transmission and/or gather data, essential for the real time operation of the BES, which if rendered unavailable, degraded or compromised, has the potential for an Adverse Reliability Impact. This definition will limit the scope to address vulnerabilities related to a cyber attack on systems that impact the real time operation of the BES. If it is the intention of the drafting team to include systems that do not directly affect real time operations, then it is our recommendation that this should be addressed in another standard(s). The NERC Glossary of Terms should be used when there are defined terms available for use. Adverse Reliability Impact is such a term.
Consumers	Disagree	This needs to be specific to at risk cyber systems. There are cyber systems that could adversely impact the reliability of the BES that are not at risk since they do not use routable protocols. The definition of critical cyber assets was more descriptive and better suited the intent of the reliability standards. This seems to simply be another way of saying the system or device is a Critical Cyber Asset (CCA) and provides no further benefit. In addition, the phrase: “has the potential to adversely impact” is too vague. For example, a device such as a controller, RTU, relay could be unavailable for an extended period of time and have an ‘adverse impact’ in that it is certainly inconvenient. However, since protection and control system operations on the BES are automatic and independent of SCADA control, loss of an RTU, for whatever reason, is not immediately or by default a critical situation. In addition, there needs to be recognition that if the devices are not networked, and access to one device cannot easily lead to other devices, the concern is minimal and therefore not critical (or a BEC Cyber System, by this definition) There appears to be a conflict of the definition with the category of a “Low” BES Subsystem as a low classification (and thus its related cyber system) cannot adversely impact the reliable operation of the BES. We are struggling to see how a classification of “Low” could possibly have a BES Cyber System which is critical to the reliable operation of the BES, so it would appear that there would never be BES Cyber Systems for Low Subsystems! Suggested definition: A Cyber System which if remotely accessed (via a routable protocol or dial-up) and rendered unavailable, degraded, or compromised has the potential to initiate, disable or compromise (through direct command or setting changes) operating functions critical to the reliable operation of the Bulk Electric System or essential for the operation of a generation unit which could adversely impact the reliable operation of the BES.
NPCC	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” The definition is not clear, creates audit issues. Needs to be more explicit on what the definition of boundaries of cyber system applicability are. (Attachment 2 to be considered).
SWPA	Disagree	A definition should focus on the meaning of the phrase, not place parameters around it such as “which if”. A more concise definition would be “A discrete set of one or more programmable electronic devices organized to control and/or monitor the real-time operation of the BES.”
MPPA	Agree	However, MPPA suggests that the term “has potential to adversely impact” may be overly broad and vague.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
Central Lincoln	Disagree	Relies in the definition of Cyber System, which itself is unclear (see 1a).
NERC	Disagree	The concept of "misuse" needs to be captured along side of the current concepts of availability, degradation and compromise
Dominion	Disagree	Dominion proposes that the definition term "BES Cyber System" be changed to "Critical Cyber System" while keeping the definition text of "BES Cyber System." This change captures the intent of the current definition, while emphasizing and clarifying the criticality of the cyber system. Dominion disagrees with the retirement of the following terms "Critical Assets," "Critical Cyber Assets" and "Cyber Assets." Revising the definition of the term "Critical Asset" would be superior to creating the new terms "Bulk Electric System Subsystem (BES Subsystem)," "Generation Subsystem," "Transmission Subsystem" and "BES Cyber System." Dominion proposes the definition of "Critical Asset" be modified to include portions of the proposed new terms "Generation Subsystem" and "Transmission Subsystem" and read: "Generation or Transmission assets (generators, substations, transmission buses, transmission lines, transformers) whose Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Dominion disagrees with the use of "Element" in the definitions of singular and aggregated basis. NERC currently defines the term "Element" as, "Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components." This definition would effectively apply to all electrical devices. Dominion recommends replacing "Element" with "Cyber System" as defined in Section 1.a above. As applied: (a) Singular basis – the failure of a single Cyber System would render the output of the asset unavailable; or (a) Combined/Aggregated basis - the failure of a shared Cyber System would result in the combined output of the assets becoming unavailable.
Encari	Disagree	Requirement R3.1 implies that any Cyber System within a BES Subsystem that is identified under the criteria in Attachment 1 has the potential to be a BES Cyber System. That may not be the case since the definition of a Cyber System is not tied or related to the definition of a BES Subsystem. In order to ensure the implied relationship exists, we recommend the definition of BES Cyber System be expanded to state, "A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. A Cyber System associated with a BES Subsystem identified under the criteria in Attachment 1 is presumed to be a BES Cyber System if the Cyber System has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System."
US ACE – NW	Agree	

Organization	Yes or No	Question 1.b. Comment (Response page 6)
SCE	Disagree	The definition should be revised to replace “has the potential” with “has significant potential.” The term “potential” is, standing alone, extremely broad and thus may unreasonably expand the scope of what should constitute a BES Cyber System. Including the term “significant” will help ensure that only Cyber Systems that may have a genuine impact on the BES will be within scope.
USBR	Agree	
Dyonyx	Disagree	We believe it is important that a draft of CIP-003-4 through CIP-009-4 be made available prior to the ballot requirement for CIP-002-4. This is crucial for Entities to understand the potential impact of the new classification prior to agreeing to all the criteria as specified in CIP-002-4. For example, currently the draft CIP-002-4 specifies that all BES Cyber Assets not classified as High or Medium will automatically be classified as Low. This means that those Cyber Security Controls specified in the CIP-003-4 to CIP-009-4 standards required for Low BES Cyber Assets would have to be applied. Consideration may be needed for an additional classification level of “Not Applicable” or some other form depending upon the extent of the requirements imposed by the Low classification.
FMPP	Agree	
MISO	Disagree	Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems “also includes all of the components necessary to ensure the protection of the reliability function(s) being performed”. If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
Westar	Disagree	The phrase 'has the potential to' is vague and leaves room for interpretation. Suggest replacing with 'will'.
Green Country	Disagree	A Cyber System organized to control and/or monitor the real time operation and support reliable operation of the BES.
Oregon PUC	Disagree	Oregon PUC Safety Reliability Security Staff believe the term “potential to adversely impact” has too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
NB Power Gen	Agree	However, the previous CIP-002 R3 (R3.1, R3.2, R3.3)defined criteria for classifying BES Cyber Systems such that it was clear which systems were vulnerable to remote attack and which were not. The previous set of cyber security standards addressed the vulnerability of cyber systems to cyber threats external to the facility, which seemed to be the premise for the security issue (remote coordinated attacks via communication links). If cyber systems are not connected in any way such that a threat external to the facility is neutralized, most of the rest of the CIP-003 through CIP-009 were not applicable (not required since there was no possibility for remote access attack). Most of the CIP-003 requirements made sense to implement to ensure continuous monitoring, change management and vigilance to ensure configuration changes introduced no new communication links that would allow external communication to BES Cyber Systems within the facility, and to ensure that there was senior management responsibility. The revised definitions are good as far as they go, but they do change the scope of the applicability of the standards to

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		include cyber systems that cannot be accessed from outside the facility. Within the boundaries of a generating station, whether single or multiple unit, if there are no external communication links that provide a means of access to BES Cyber Systems, whether wired or wireless, there should be no need to implement the security measures required by CIP-004 through CIP-009 for the purpose of securing the BES Cyber Systems from a remote access threat. I suggest that unless the intent has changed (i.e., now we need to protect BES cyber systems that may have impact on the BES reliability from any physical access attack within the facility instead of from remote access external to the facility) that the revised CIP-002 should include a further definition that limits the scope of applicability of the security measures to those BES Cyber Systems that have any communication link outside of the facility that allow communication to BES Cyber Systems within the facility. Alternatively, leave the definitions as currently proposed and in the other CIP Standards, allow for the isolation of BES Cyber Systems from communication access outside of the facility as a security measure that is an accepted approach to compliance. This would require appropriate documented configuration change management for ongoing vigilance.
Manitoba 1	Agree	
Wolverine	Agree	
Portland GE	Disagree	The term “potential to adversely impact” has too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
PSEG	Disagree	Comment #1: We disagree with this definition because it is not clear as to the meaning behind the phrase “adversely impact functions critical to the reliable operation of the BES”. Comment #2: A Transmission Subsystem which is identified as “Low” could not by definition have an impact on BES Cyber System (using the proposed definition)? The definition of “Low” is something that can not adversely impact the reliable operation of the BES. (Conclusion: A classification of “Low” can not have a BES Cyber System which is critical to the reliable operation of the BES.”) Comment #3: We strongly recommend that the SDT delete the word “critical” from the definition of BES Cyber System. Comment #4: We recommend that we retain the CCA terminology Comment #5: This needs to be specific to at risk cyber systems. There are cyber systems that could adversely impact the reliability of the BES that are not at risk since they do not use routable protocols. The definition of critical cyber assets was more descriptive and better suited the intent of the reliability standards. Suggestion: A Cyber System, contained within an Electronic Security Perimeter (ESP), that if compromised (through an electronic interface) has the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch, relay or tap changer), interrupt a generating unit’s production capability or disrupt / corrupt real-time data.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		Our proposed definition provides the necessary clarity as to what Cyber Systems need to be included the classification of a BES Cyber System(s). We agree with the use of the acronym Bulk Electric System (BES) for this term. This clarity is needed to reinforce that NERC's jurisdiction provided under FPA 215 includes only those facilities that fall under the definition of Bulk Electric System. Bulk Electric System as defined by NERC: "As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.
Idaho Power	Agree	
SOCO	Disagree	The phrase: "has the potential to adversely impact" is too vague. For example, a RTU could be unavailable for an extended period of time. That will be an adverse impact in that it is certainly inconvenient. However, since protection and control system operations on the BES are automatic and independent of SCADA control, loss of an RTU, for whatever reason, is not immediately or by default a critical situation. Another example is primary and secondary protective systems; the loss of one or the other but not both simultaneously is not immediately a critical situation. Suggest the following definition: A Cyber System which if rendered unavailable, degraded, or compromised will immediately impact functions critical to the reliable operation of the Bulk Electric System such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures. Suggested definition: A Cyber System which if remotely accessed and rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System or essential for the operation of a generation unit which could adversely impact the reliable operation of the BES. The phrases "essential to operations" and "routable protocol" should be added to the BES Cyber System definition.
DTE	Agree	
AEP	Disagree	In combination with the "Cyber System" definition above, this definition becomes more problematic. The Cyber System definition does not provide sufficient detail as to the level of sophistication of the devices that are at risk and that need to be protected. Given that a system is made up of a collection of parts, each part does not create the same degree of impact to the BES. This draft standard collectively groups the parts, then groups the facilities, and then determines the impact of any single part based on the highest possible impact. This may well have the unintended consequence of

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Disagree	See previous answer. We agree with the idea of distinguishing computerized systems that perform or support functions necessary for BES reliable operations from those that do not. However, we are concerned about how "far" or "deep" one must go in order to identify computerized systems with the "potential" to adversely impact the BES. This is not a new problem; popular examples include HVAC systems and coal conveyors that operate under computerized control. Must they be counted as BES Cyber Systems? Should business systems that play a role in Entity operations be included? The real-world answer is probably, "It depends." We believe NERC and the SDT may *have* to come down on one side or the other of this kind of question if the goal of establishing "bright lines" is to be achieved.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently.
E ON	Disagree	As described above, the definition of “Cyber System” is far too inclusive. E ON U.S. would urge the drafting team to keep in mind the purpose of the cyber security requirements, that is to prevent unauthorized electronic access to mission critical programmable devices. The re-write of CIP-002 appears to drop language in the previous versions that address assets connected via a “routable protocol.” In fact, connectivity to a cyber asset doesn’t seem to be addressed at all, leading to the concern that standalone assets, those not connected to any network, could be brought into scope through association with a high or medium rated BES subsystem. Accessing stand alone devices requires an intruder’s physical presence and connecting with proprietary interface. An intruder could far more easily operate control panel switches and thus the preventing physical unauthorized access should remain the objective. Absent the ability to remotely connect and communicate, a standalone programmable device should not be considered a Cyber Asset for purposes of these standards. There also remains ambiguity regarding network perimeter devices such as firewalls, routers, and the like. Should these devices be treated as separate perimeter devices and not part of a BES cyber system?
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	An “element” or “component” of a cyber system if compromised or not properly maintained could have the same effect.
CenterPoint	Disagree	Disagree – See comments on 1.a. This definition is very broad and would seem to describe the already accepted and understood term of a critical cyber asset.
CA Cogen	Disagree	Our concern with Version 4 is that it removes any determination of whether a cyber asset is accessible from outside the

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		facility. Versions 1-3 require that a cyber asset have either routable protocols or dial-up access. These limitations are important because they indicate whether the cyber asset is vulnerable. If it isn't vulnerable, then it should be treated as any other part of the equipment of the facility. These requirements for accessibility should be included somewhere in the standard. Perhaps in the global re-working of the CIP standards, they will be included somewhere else, but they could possibly be included in the definition of "BES Cyber System."
LCRA	Agree	
FRCC	Disagree	What do the terms degraded and compromised mean? They are ambiguous terms and could have many different meanings depending on who you ask. I believe there has already been an interpretation request in 2009 that sought guidance to the term degraded so this is not new. These kinds of terms should not be used in a definition or a requirement in a Reliability Standard. If the drafting team has an understanding of what they mean, they should explicitly state it and not use such ambiguous terms.
NIPSCO	Disagree	We are concerned that it is unclear as to the meaning behind the phrase “adversely impact functions critical to the reliable operation of the BES”. Suggestion: Further clarifications on the intent of this language is needed.
ConEd	Agree	
EEI	Disagree	Alternative Definition: A Cyber System, with the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch or tap changer), interrupt a generating unit’s production capability or disrupt / corrupt real-time data.
O&R	Agree	
Alliant	Disagree	We believe the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose "A Cyber System associated with the operation of a Bulk Electric System Subsystem.
Ameren	Disagree	A Cyber System should be replaced with “A Responsible Entities’ Cyber System”. To make it clear that this only includes Cyber Systems under the control of the Responsible Entity and specifically excludes entities such as Verizon. What is meant by "adversely impact"? This term could include almost anything, and needs to be more narrowly defined. We recommend replacing “has the potential to adversely impact” with “would be unable to perform”. Also, the phrase "has the potential to" needs to removed and changed to "will". We need to get away from the hypothetical and focus on the more concrete issues.
Black Hills	Agree	The definition itself is technically sound, but its implication is profound because virtually all Cyber Systems have some "potential" (unqualified) to "adversely" (unqualified) impact reliable operation of the BES.
TNMP	Disagree	TNMP believes the Cyber System definition needs to be revised for clarity as discussed in the response to 1.a. Also the

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		phrase “has the potential to adversely impact functions critical” lends a prejudice that a BES Cyber System has a High BES Impact. A change to “has the potential to have a high, medium, or low impact on functions critical to the reliable operation of the Bulk Electric System” would maintain the concept of potential impact while allowing for the importance to be defined by a High/Med/Low BES Impact label.
NVEnergy	Disagree	Given the remarks in 1.a above, we recommend that the term Cyber System be changed to Cyber Device or Cyber Asset.
MWDSC	Disagree	"Potential to adversely impact functions critical" is too vague. Doesn't consider systems which can be unavailable, but do not impact functions because of redundancy or other reasons.
Empire	Disagree	Option to redefine BES Cyber System to: A discrete set of one or more programmable electronic devices that operate BES devices at 200 kv and above to control and/or monitor the real time operation of the BES
NCEMCS	Agree	Not all cyber systems would have an impact. The cyber system must be in direct support of the BES or have some cascading (impact other systems that direct support of the BES) impact.
BCTC	Disagree	See Question 13
SWTC	Disagree	Not so much with BES Cyber System Definition. Here again the BES needs to be defined.
SCEG	Agree	
Exelon	Disagree	In addition to concerns about the possible overlap and or conflict between definitions used by the various regulatory entities, as the largest owner/operator of nuclear power plants in the United States we have concerns about the potential of duplication of efforts. Currently nuclear power plants employ very strict and thorough physical and cyber security controls and urge NERC to consider those protocols as the CIP standards are developed to avoid needless duplicative efforts As a result Exelon asks the SDT to consider the following revised BES Cyber System definition:. A Cyber System which if rendered unavailable, degraded, or compromised via cyber attack has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.
BPA Trans	Disagree	The Cyber System is not adversely impacting functions, its loss, degradation or compromise is. Our proposed modification would be: “A Cyber System whose compromise, degradation, or loss of availability has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.”
HQT	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” The definition is not clear, creates audit issues. Needs to be more explicit on what the definition of boundaries of cyber system applicability are. (Attachment 2 to be considered).

Organization	Yes or No	Question 1.b. Comment (Response page 6)
CCG	Disagree	Page 7 of the guidance document defines BES Cyber System and then states “This definition includes all of the components necessary to ensure the protection of the reliability functions being performed.” This addition to the definition is overly broad and inappropriate. If the definition of BES Cyber System needs to be changed to include additional components, it should be performed through the stakeholder process. There should not be additional items brought into the definition through the guidance document.
Allegheny Supply	Agree	
KCPL	Disagree	No, the definition for a BES Cyber System should not be conditional on the impact a cyber element may or may not have on the BES. This should identify the systems to be examined and the process should determine the criticality and need for appropriate security protections. I believe acceptance of this notion would effectively make the definition for “Cyber System” and “BES Cyber System” identical and, therefore, one of them could be eliminated.
Connectiv Energy	Disagree	Concerned with use of the words “potential to adversely impact…” This leaves a lot to interpretation, and if conservatively considered most cyber systems have the ‘potential’ to adversely impact a function. Adversely Impact to what degree? A minor impact may not be of concern but would meet this definition.
MidAmerican	Disagree	See comments to 1.a. on Cyber System. If Cyber System and BES Cyber System definitions are proven to be needed for categorization of security controls, the definition should be “Cyber Systems controlling BES Facilities.” This eliminates the issues of the broad, undefined concept of “potential to adversely impact functions” in the draft CIP-002-4 definition.
CPG	Disagree	For the purposes of defining a BES Cyber System, the Cyber system explanation should be combined into the BES Cyber System definition. The definition of BES Cyber System should read, “A discrete set of one or more programmable electronic devices organized for the collection, processing, maintenance, use, sharing, or communication of data, which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.” There should also be further distinction between those systems attached to routable networks and those that are not.
Santee Cooper	Agree	
OGE	Disagree	• This statement could be improved if we had something more definitive. The term "potential" is quite subjective and open to interpretation. • OPTION: A discrete set of one or more programmable electronic devices organized to control and/or monitor the real time operation of the BES.
Oncor	Disagree	Do not assume an adverse impact. Restated- “A Cyber System associated with the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
PPL Supply	Disagree	The subject definition should be clarified to exclude “market systems.” The potential inclusion of “market systems in the definition of BES subsystems and BES Cyber Systems seems to be overly broad. In general, these "market systems" allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market, among other things. An overly broad definition could end up including these "market systems" under the purview of the CIP standards which could result in increased burdens with little or no resulting increase in reliability.
St. George	Agree	
NGRID	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” Also, the phrase “adversely impact functions critical to the reliable operation of the BES” is confusing since as per the proposed definitions of Transmission/Generation subsystems, anything identified as “low” could not by definition have a BES Cyber System, that is, a classification of “Low” can not have a BES Cyber System which is critical to the reliable operation of the BES. National Grid recommends deleting the word “critical” from the definition.
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to Cyber Systems of 100kV or greater. The use of the words “potential to adversely impact” and “critical” will leave all entities and users, owners, or operators of the BES and regulators the ability to interpret this as outside the scope of the SDT definition. Recommend that BES Cyber System read as: A BES Cyber System which if rendered unavailable, degraded, or compromised will have a direct impact on maintaining equipment or electric system’s thermo, voltage and stability limits where as instability, uncontrolled separation, or cascading failures that directly impact the reliable operation of the Bulk Electric System.
FE	Agree	
TECO	Agree	We agree with this definition, however, we do not believe the standard as currently worded accomplishes this.
CECD	Disagree	The definition references an undefined term "critical functions" which will have a significant impact on whether a Cyber Systems will be identified as a BES Cyber System, and CECD encourages the drafting team to either include a definition or a specific reference to clarify what the critical functions are or clearly state that these functions can be identified by the registered entity. In this draft, Attachment 2 entitled "Functions Critical to the Reliable Operation of the BES" is intended to define this term so there should be a reference to that Attachment if this is the direction the drafting team is taking. CECD does not agree that all of the functions described are critical (the language is too inclusive) and we would prefer to define what is a critical function for our operation, in coordination with our neighbors as appropriate.
MRO	Disagree	We feel the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose “A Cyber System associated with the operation of a Bulk Electric System Subsystem”.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
GTC	Disagree	If "functions critical to the reliable operation of the Bulk Electric System" is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2. The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
Xcel	Disagree	We feel the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose "A Cyber System associated with the operation of a Bulk Electric System Subsystem".
BGE	Disagree	We believe that for the purposes of defining "BES Cyber System" the "Cyber System" explanation should be rolled into 1.b. The definition of BES Cyber System should read, "A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System." We believe there may be further distinction required between BES Cyber Systems attached to routable networks vs. those that are not. This is because there can be a wide range of appropriate protective measures commensurate with the risks associated with those systems.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although we agree that a BES cyber system affects the reliability of the BES, this definition should include more detail on what is meant by unavailable, degraded, or compromised as there may be back-up systems to help mitigate these problems.
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	AP disagrees with this definition because it is not clear as to the meaning behind the phrase "adversely impact functions critical to the reliable operation of the BES".
FMPA	Disagree	The NERC Glossary of Terms should be used when there are defined terms available for use. Adverse Reliability Impact is such a term. Hence, the definition should read: "A Cyber System, which if rendered unavailable, degraded or compromised, has the potential for an Adverse Reliability Impact." There is no need to add the term "functions" to the definition. A results-oriented, performance based standard would

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		simply care if there is a potential for an Adverse Reliability Impact. The addition of the concept of functions is confusing and we do not see significant added value. For instance, how are these "functions" different than the "Functional Model"?
Duke	Disagree	Definition should be revised to remove ambiguous language. Suggested wording: BES Cyber System – A Cyber System which has the potential to impact reliable operation of the Bulk Electric System.
AESI	Disagree	If "functions critical to the reliable operation of the Bulk Electric System" is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2. The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
IESO	Agree	
Manitoba 2	Disagree	Please define "degraded" as it applies in this definition. "Potential to adversely impact functions" should be changed to "will adversely impact functions". In the document DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems, the section "What is a Cyber System" includes "infrastructure support components – devices supporting the confidentiality, … of the BES Cyber System…" in the definition of the BES Cyber System. The primary issues to support the reliability functions are integrity and availability. Including confidentiality makes the scope of cyber systems requiring protection overly broad. It is unclear how to define the boundaries or breadth of a BES Cyber System. Are cyber systems which primarily support a maintenance activity related to a BES Subsystem to be included in the scope of this definition? If, so how is it limited to the most important activities? "Functions critical" is not defined, and should not be referenced in this definition. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	OMPA does not agree that every BES cyber system has the potential to adversely impact functions critical to the reliable operation of the BES. OMPA urges the drafting team to consider a fourth, "no impact", option for those cyber systems that do not have the potential for adversely impacting the real-time operation of the BES. This definition assumes all BES cyber systems have the potential to adversely impact the reliable operation of the BES.
ATC	Disagree	ATC disagrees with this definition because it is not clear as to the meaning behind the phrase "adversely impact functions

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		critical to the reliable operation of the BES". A Transmission Subsystem which is identified as "Low" could not by definition have a BES Cyber System (using the proposed definition)? The definition of "Low" is something that can not adversely impact the reliable operation of the BES. (Conclusion: A classification of "Low" can not have a BES Cyber System which is critical to the reliable operation of the BES.") ATC strongly recommends that the SDT delete the word "critical" from the definition of BES Cyber System. Suggestion: A Cyber System, contained within an Electronic Security Perimeter (ESP), that if compromised (through remote access) has the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch or tap changer), interrupt a generating unit's production capability or disrupt / corrupt real-time data. ATC's proposed definition provides the necessary clarity as to what Cyber Systems are to be included in the classification of a BES Cyber System(s). ATC does agree with the use of the acronym Bulk Electric System (BES) for this term. This clarity is needed to reinforce that NERC's jurisdiction provided under FPA 215 includes only those facilities that fall under the definition of Bulk Electric System. Bulk Electric System as defined by NERC: "As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.b. Comment (Response page 6)</th></tr>
<tr><td></td><td></td><td>
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>
BES Cyber system: Cyber system essential to the reliable real time operation of Bulk Electric System which if rendered unavailable, degraded, or compromised has an Adverse Reliability Impact.
Adverse Reliability Impact is already a defined term in the NERC Glossary.
It is unclear whether BES Cybersystem encompasses the assess control, monitoring, and logging systems that were
</td></tr>
</table>

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		previously treated differently in versions 1 and 2/3 or whether they will be treated separately within the CIP-003 through CIP-009 revisions. We suggest more clarity regarding the definition of a BES Cybersystem as it could be interpreted to include HVAC, Communications systems, and even IP addressable power strips. Also the terms “potential”, “adverse” are again terms that are open for interpretation.
IMPA	Disagree	IMPA proposes the following definition for BES Cyber System. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to have an Adverse Reliability Impact to the reliable operation of the Bulk Electric System.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. The definition and consideration points used in the Guidance are more comprehensive in evaluating the various types of systems used to support reliability functions and should be the definition used. Additionally, the use of redundant components should be addressed in the definition particularly where the redundant components fully provide the same functionality of the primary system. Midwest ISO Comments: Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems “also includes all of the components necessary to ensure the protection of the reliability function(s) being performed”. If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
PacifiCorp	Disagree	If Cyber System and BES Cyber System definitions are proven to be needed for categorization of security controls, the definition should be “Cyber Systems controlling BES Facilities.” This eliminates the broad, undefined concept of “potential to adversely impact functions” in the draft CIP-002-4 definition.
PEPCO	Disagree	The draft definition is not clear and seems to be subject to interpretation. A clearer definition of - if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation. What is considered - adversely impact? What is meant by critical to the reliable operation? Does the fact that critical is used in the definition mean that it has to be a high impact system? The overall definition needs to be bright-lined. We suggest the following: BES Cyber System: An electronic cyber system with the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (e.g. circuit breaker, switch or tap changer), interrupt a generating unit’s production capability, or disrupt / corrupt real-time electric operations data.
NEI	Disagree	A) Clarification of the terms “degraded”, “compromised”, “potential to adversely impact” and “critical to the reliable operation” is required. B) NEI suggests that the definition be simplified to “A cyber system (or element or component thereof) that has the potential to impact the reliable operation of the BES.” C) In combination with the proposed “Cyber System” definition, this definition becomes more problematic. The Cyber System definition does not provide sufficient detail as to the level of sophistication of the devices that are at risk and

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		that need to be protected. Given that a system is made up of a collection of parts, each part does not create the same degree of impact to the BES. This draft standard collectively groups the parts, then groups the facilities, and then determines the impact of any single part based on the highest possible impact. This may well have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Summary Consideration:

Organization	Yes or No	Question 1.c. Comment (Response page 7)
Progress Energy	Disagree	NERC needs to fully define “BES Facilities” in order for this definition to be useful.
EPSA	Disagree	Current BES Subsystem definition is unclear thereby consistent identification will prove difficult. In 1.1 Aggregated Rated Name Plate and 1.2 Aggregate Output do not distinguish if the aggregate nameplate generation at a node, regardless of facility ownership or the generation controlled by a distinct control system. EPSA believes the control system can indeed have sufficient controls without every generating facility connected to it being identified as part of the Subsystem. In addition, Reserve Sharing Obligation does not distinguish whether this is for a specific Generation facility or the Balancing Authority as a whole. This is also true for Contingency Reserve.
GSOC/OPC	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say “A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center.” Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
Hayden	Disagree	1. Add to the end of the sentence "...on the Bulk Electric System (>100 kv)." This is added to ensure that we are not addressing generation facilities used on distribution systems or non-BES facilities.
SDGE	Disagree	We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used in the generation or transmission of energy.
APPA	Disagree	BES Subsystem: Subsystems add an unneeded step and add confusion The SDT can get to the same classification analysis by both defining subsystems and then determining their impact on the BES, or starting directly with the worst case scenario analysis of a malicious use of a cyber system. We question the purpose of adding the step of defining Subsystems to the analytical process, which seems unneeded. Since the draft does not describe how groups of Facilities are to be categorized into cyber systems, then it will be difficult to determine if the groupings developed by a registered entity are technically correct and auditable. We envision a situation where compliance authority auditors disagree with the registered entity on how Facilities are to be grouped into subsystems, without any clear requirements to guide such classifications. We also anticipate that we would get into the same situation where each entity is allowed to define its subsystems by a methodology determined by the entity. This

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		categorization process has the potential for subjectivity that the proposed bright line criteria were intended to reduce or eliminate. We believe it is simpler, more straightforward and less confusing to skip the step of defining subsystems and simply ask registered entities to map their cyber systems' control paths to and data paths from their BES systems. This mapping is performed by asking the question: What's the worst case scenario that can be caused by a malicious use of a cyber system? What would be the "Adverse Reliability Impact" of that cyber system? If the SDT chooses to retain the concept of Subsystems, which we believe adds unnecessary complication and confusion, we recommend grouping by the scope of a Cyber System and eliminating the phrase "or ensure the ability to . . ." which is either redundant or overly inclusive of non-BES facilities. The resulting definition would read: "A group of one or more Facilities (such as a Generation Subsystem, Transmission Subsystem, or Control Center) used to generate energy, transport energy that share a common Cyber System."
Consumers	Disagree	Again, this seems to simply be another way (and again with no benefit or additional clarity) of referring to Assets. See Section 13.
NPCC	Disagree	The existing use of Facility is inconsistent with the definition in the NERC Glossary and excludes some subsystems in Attachment 1 Recommend that the definition is "one of Generation Subsystem, Transmission Subsystem, Control Center, Protection System, and SPS, RAS or automatic load shedding." Recommend this definition follow 1.f Control Center.
SWPA	Disagree	The use of the term "ensure" in this context is improper. It is not possible to "ensure" that the thousands upon thousands of mechanical parts which make up the BES will continuously be available for the generation or transportation of energy. This is simply beyond the ability of any registered entity. Suggest replacing with "A group of one or more BES facilities controlled and/or monitored by a common BES cyber system."
MPPA	Agree	Language could be added to more clarify that these standards apply to those systems above 100 kv.
Central Lincoln	Disagree	Definition relies on the definition of the BES, which is not understood and is inconsistently interpreted across the regions. Continuing to use a flawed definition to define others only increases the ambiguity. Suggest NERC and/or the regions finish the BES definition work before building further on top of it. Suggest removing the word "system", so that we don't have the redundant "system subsystem" in the defined term.
Dominion	Disagree	See comments to 1.b.
Encari	Disagree	We further recommend that "BES Subsystem" refer to asset types with minimal thresholds for materiality. For example, "generation plant" could be replaced by the term, "generation resource that meets the criteria for inclusion in the NERC compliance registry." Absent materiality thresholds, a SCADA system that controls two wind powered generator units,

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		each at separate locations, with a combined generation capacity of 10,000 kWh annually, could be considered a control center.
US ACE – NW	Agree	
SCE	Agree	
USBR	Agree	
Dyonyx	Disagree	The structural intent of the BES Subsystem, Generation Subsystem, Transmission Subsystem, and Control Center terms conceptually appears to be quite appropriate. However, the definition of the terms "used in the definitions" is very confusing. First, the term "BES Subsystem" itself is a confusing use of the word "subsystem". The proposed definition for the "BES Subsystem" uses the phrase a "group of one or more BES Facilities…." Why not go ahead and use the term "BES Facility" and define it as "A group of one or more Generation Subsystems, Transmission Subsystems, or Control Centers used to generate, transport energy or ensure the ability to generate or transport energy"? The use of the recommended term "BES Facility" is a separate definition from "facility" in the NERC Glossary of Terms and in our opinion the former is more appropriate for use herein.
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to ensure the ability to generate or transport energy.
Oregon PUC	Disagree	The term "ensure the ability to generate or transport energy" is too broad and leaves too much room for auditor and enforcement interpretation. Clear, specific and technically defensible language is needed for this definition.
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	The term "BES Facilities" needs to be defined.
PSEG	Disagree	Comment #1: The terms Generation Subsystem, Transmission Subsystem and Control Center seem to provide the necessary granularity to effectively convey the SDT intentions of this definition. We believe that this definition is not required and therefore should be deleted. Comment #2: We are concerned about the use throughout these documents of the words Facilities, Elements, and subsystem. These do not appear in the glossary and in some cases appear confusing and potentially conflict with those

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		interpretations used in other NERC standards: TPL, FAC, EOP, etc.
WE-Energies	Disagree	The definition of BES Subsystem includes the vague statement “or ensure the ability to generate or transport energy." This is unnecessary and should be deleted.
Idaho Power	Agree	
SOCO	Agree	
DTE	Disagree	Since this term is used in the standard as a combination of the next three terms, Generation Subsystem, Transmission Subsystem, and Control Center consider changing it to the following to avoid repetition and confusion. Bulk Electric System Subsystem (BES Subsystem) — A Generation Subsystem, Transmission Subsystem, or Control Center.
AEP	Disagree	Defining groups of BES facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Disagree	The structural intent of the BES Subsystem, Generation Subsystem, Transmission Subsystem, and Control Center terms conceptually appears to be quite appropriate. However, the definition of the terms “used in the definitions” are very confusing. First, the term “BES Subsystem” itself is a confusing use of the word “subsystem”. The proposed definition for the “BES Subsystem” uses the phrase a “group of one or more BES Facilities….” Why not go ahead and use the term “BES Facility” and define it as “A group of one or more Generation Subsystems, Transmission Subsystems, or Control Centers used to generate, transport energy or ensure the ability to generate or transport energy”? The use of the recommended term “BES Facility” is a separate definition from “facility” in the NERC Glossary of Terms and in our opinion the former is more appropriate.
Calpine	Agree	
NS&T	Disagree	We believe the goal of allowing flexibility in how Entities define their "BES Subsystems" has resulted in a definition with too many degrees of freedom, and that the result could be disproportionate amounts of time spent on how to draw "subsystem" lines around BES assets, to the detriment of improving cyber security.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently.
E ON	Disagree	After reviewing Attachment 1, E ON US surmises that the category “ensure the ability to generate or transport energy”

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		refers to Control Centers. E ON U.S. recommends it be stated as Control Centers to avoid ambiguity.
Carthage		CWEP would like better clarification on BES Subsystems. Is the standard referring to the BES as defined in the NERC Glossary? If so, are entities with no facilities or assets that operate at 100 kV and higher meant to be exempt?
WECC	Disagree	Not sure that we need this additional level of definition. Something is either part of the BES or not and it is redundant with the definition of generation, transmission, and control center following.
Entergy	Disagree	Doesn't translate well in practical terms to aid Entities identify what needs to be protected. Examples: How do cranking paths translate into "subsystems" and/or "facilities?" Generation-Transmission interconnection methods vary widely, not always including a "switchyard" per se, and are often comprised of assets owned/operated by more than one Entity – how do the various scenarios equate with subsystems and/or facilities? What about special protection schemes – subsystems and/or facilities? These challenges in definition highlight the incongruity in attacking the issue of cyber security using primarily a grid electrical engineering frame of reference versus that of networked computing systems engineering. Square peg, round hole.
CenterPoint	Disagree	Disagree – See comments on 1.a and 8. This definition could create auditable implementation confusion due to the interconnected nature of the BES. For example, ten power plants could be a "subsystem", or could represent two "subsystems" of five power plants each, or three "subsystems" adding up to the ten power plants, or various other combinations. Alternatively, the ten power plants plus "connecting" transmission assets (which could be defined in multiple ways since the entire BES is interconnected) could be a "subsystem". Moreover, subsystems that "ensure the ability" to generate or transport energy could be construed in multiple ways to include or not include such things as fuel pipeline systems, for example. Since a pipeline system is generally a common carrier system outside the control of the responsible entity, the question then becomes how many of the pipeline assets should be construed as the "BES subsystem"? In short, the proposed definition creates confusion without appearing to add anything of value.
LCRA	Agree	
FRCC	Disagree	I do not believe that the definition helps and in fact if you look at R1 where the application of the criteria in attachment 1 is required, you really do not need to have the definition of BES Subsystems. The criteria are pretty clear and this definition does not help.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility within the proposed definitions.
ConEd	Agree	

Organization	Yes or No	Question 1.c. Comment (Response page 7)
EEI	Disagree	Differentiating between high, medium and low Bulk Electric System Subsystem may have little value or credibility for associated cyber security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
O&R	Agree	
Alliant	Agree	
Ameren	Agree	None
Black Hills	Disagree	The definition (size-wise) of what must constitute a "subsystem" is not defined, and therefore would be relative to the interpretation by the entity (some of which could be very large or very small).
TNMP	Disagree	Using the phrase “a group of one or more BES Facilities” permits multiple possible constructs of BES Subsystems owned by a Responsible Entity. A BES Subsystem could be a comprised of a number of substations along a critical path transmission path or cranking path. If the drafting committee is looking to move forward with the concept of ”one or more BES Facilities” then a better definition or criteria of when it applies to multiple BES Facilities is needed to give the standard “bright lines”. Also, the definition refers to “BES Facilities,” but neither the proposed standard nor current NERC glossary contain this term. Either the phrase needs to be officially defined or removed from the definition.
NVEnergy	Agree	
MWDSC	Disagree	Unclear whether the term "BES" has been accepted as a NERC defined term instead of "Bulk Power System". What about regional differences in defined BES? A BES Subsystem may be isolated and not affect other interconnected systems. For example, if you have one generator with a radial line to a load, it wouldn't affect any other system. Wouldn't the standard require a "low impact" assessment with unknown cyber security measures?
Empire	Disagree	Optional definition: BES Subsystem: A group of one or more BES Facilities controlled and/or monitored by a common BES Cyber System
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	The definition of a BES Subsystem again goes back to what is the BES.
SCEG	Agree	We agree with the definition, however we feel that the SDT needs to ensure that any subsystem which does not meet one of these three defined categories is defined.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
Exelon	Agree	Although Exelon agrees with this definition, as stated previously Exelon has concerns with the proposed CIP standard definitions that may result in overlaps and/or conflicts in definitions between the regulatory entities (NRC, CNSC, and NERC). We ask that NERC and/or the SDT take action to ensure the proposed definitions are reviewed and revised if needed to eliminate any potential overlaps. In addition Exelon is hoping for a timely and clearly stated scope of applicability from the NRC to U.S. nuclear plant owners/operators. As currently drafted the system/subsystem concept and the Attachment 1 criterion without the scope of applicability will likely create confusion as NERC and the SDT attempt to define the standards. The industry will likewise have difficulty as they attempt to understand and comply with the CIP standard requirements.
BPA Trans	Disagree	The term “BES Facilities” needs to be defined.
HQT	Disagree	The existing use of Facility is inconsistent with the definition in the NERC Glossary and excludes some subsystems in Attachment 1 Recommend that the definition is “one of Generation Subsystem, Transmission Subsystem, Control Center, Protection System, and SPS, RAS or automatic load shedding.” Recommend this definition follow 1.f Control Center The standards are written as if there is one easily defined set of BES Subsystems. This is not the case. From the cyber perspective alone there could be a different set of BES Subsystems for each type of cyber subsystem.
Allegheny Supply	Agree	
KCPL	Disagree	No, with appropriate definitions for the Generation and Transmission Subsystem, this is redundant and does no more to advance the clarity and focus of the CIP Standards to identify the components and physical facilities under consideration for cyber protection.
Connectiv Energy		
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13. This definition is not needed at this time. The necessity of this definition is caused by CIP-002-4’s proposed framework to use categorization of “iron” (substations and generating units) to categorize security controls for Cyber Assets, which are very different from “iron.” If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time, including the relevance of the associated Attachment 1. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
CPG	Disagree	This definition is not needed as the Generation, Transmission, and Control Center definitions are sufficient by themselves.
Santee Cooper	Disagree	It would seem to suggest that a BES Subsystem is a category underneath the BES Cyber System. Why not define the BES at a higher level, and forego the BES Subsystem.
OGE	Disagree	• Please provide a definition of "shared element". • What is the definition of Bulk Electric System Subsystems for generation plants and transmission systems? Can you provide examples? • OPTION: A group of one or more BES Facilities controlled or monitored by a common BES Cyber System. • The terms "transport energy" should be "transport electricity"
Oncor	Disagree	BES Subsystem appears to be a term used elsewhere in the standard to refer to Generation Subsystem, Transmission Subsystem or Control Center. If this is true, restate- "refers to Generation Subsystem, Transmission Subsystem and/or Control Center."
PPL Supply	Disagree	Please see comment in response to question 1.b.
St. George	Disagree	Every BES Facility should be specifically listed to avoid ambiguity.
NGRID	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center provide the necessary granularity to effectively convey the SDT intentions of this definition. National Grid believes that this definition is not required and therefore should be deleted. BES Electric System does not align with the terms (transmission/generation subsystems) used in Attachment 1. Also, other subsystems mentioned in Attachment 1 - Protection System, SPS will usually fall under Transmission/Generation subsystems so there is no need to mention them as "subsystems".
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to BES Subsystem(s) of 100kV or greater and the three components that that make up the BES Subsystem (Generation Subsystem, Transmission Subsystem, and Control Center). This definition is not required and should be removed since Generation Subsystem, Transmission Subsystem, and Control Center are clearly defined.
FE	Agree	
TECO	Agree	

Organization	Yes or No	Question 1.c. Comment (Response page 7)
CECD	Disagree	One of the defining lines for determining if an entity is a BES user, owner or operator is whether the equipment is operated at 100 kV or above. A generation subsystem or a transmission subsystem has one line diagrams by which the connectivity can be evaluated. A control center is more appropriately considered a Cyber System to be evaluated in relation to BES Generation or Transmission Subsystems. CECD is in favor of supporting a definition of BES subsystem that keeps enough flexibility for the registered entity to define their BES subsystems, including the ability to exclude a control center as a BES Subsystem.
MRO	Agree	N/A
GTC	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say “A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center.” Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
Xcel	Agree	
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. We recommend the following definition: Bulk Electric System Subsystem (BES Subsystem) A group of one or more BES Facilities (i.e., Generator, generator step-up transformer, transmission line, substation transformer, bus(es), and associated switches, breakers, capacitors, reactors, static var compensators, transmission control center, generator control center, market operations center used to generate energy, transport energy or ensure the ability to generate or transport energy.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center seem to provide the necessary granularity to effectively convey the SDT intentions of this definition. AP believes that this definition is not required and therefore should be deleted.
FMPA	Disagree	The process laid out in the standard is to group Facilities into “BES Subsystems”, then define the impact of that subsystem while considering the functionality of the control systems and BES subsystems. FMPA believes this whole process to be more complicated than necessary and fraught with ambiguity in defining subsystems and functions. FMPA believes these steps are unnecessary and we can get to the same point by asking ourselves “what is the worst case contingency / scenario that can be caused by malicious use of a cyber system” and use this worst case analysis against the High, Medium and Low impact framework laid out by the SDT. By doing so, we eliminate the need to define

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		subsystems and functions. An example of ambiguity in the concept of subsystems is how are Facilities grouped into subsystems? Are responsible entities supposed to develop subsystems of any combination (e.g., an almost infinite variety) of Facility groupings? Do the Elements have to be connected to each other? Do they have to be all controlled by the same cyber system? Is there opportunity for disagreement between the entities and compliance enforcement on the definition of subsystems? So far, no one has been able to tell us clearly what a subsystem is, so, that is telling in and of itself. If the SDT insists on retaining the concept of subsystems, then this ambiguity needs to be clarified. For instance: “A group of one or more Facilities used to generate energy, transport energy or ensure the ability to generate or transport energy that share a common Cyber System.” Also, for clarity, the terms BES Subsystem and BES Facility are redundant. The NERC Glossary defines a Facility as: “(a) set of electrical equipment that operates as a single Bulk Electric System Element;” hence, by definition, a Facility is part of the BES. And, since a BES Subsystem is a grouping of Facilities, which by definition are part of the BES, then the Subsystem by definition is part of the BES and the term can be simplified to “Subsystem”.
Duke	Disagree	Definition should be revised to remove ambiguous language. Suggested wording: Bulk Electric System Subsystem (BES Subsystem) – A group of one or more BES Facilities (i.e. Generation Subsystem, Transmission Subsystem, and Control Center).
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say “A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center.” Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
IESO	Disagree	Replace the word "energy" with the word "electricity". The word energy is too broad for the scope of these standards. The word electricity is also consistent with the term BES.
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	OMPA is concerned that the draft guidance for the electric sector paper allows the definition of BES subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. This could lead to subjectivity; specifically with respect to the auditing process and auditor interpretation. OMPA prefers mapping control and data paths from identified BES systems.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
ATC	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center provide the necessary granularity to effectively convey the SDT intentions of this definition. We believe that this definition is not required and therefore should be deleted.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		<table><tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr></table> Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
PSE	Agree	
IMPA	Disagree	IMPA recommends the replacement of the word “ensure” with the words “assist in”. The word ensure means “to make certain, sure, safe – guarantee”. There is no guarantee that with a Control Center in place, utilities will have the ability to generate or transport energy. A Control Center can assist with these functions but cannot ensure them.
ERCOT	Disagree	Request clarification if this grouping may span multiple locations. BES Facilities is not a defined term and should not be capitalized as such.
PacifiCorp	Disagree	See PacifiCorp’s summary comments in question 13. This definition is not needed at this time. The necessity of this definition is caused by CIP-002-4’s proposed framework to use categorization of “iron” (substations and generating units) to categorize security controls for Cyber Assets which are very different from “iron.” If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time, including the relevance of the associated Attachment 1. PacifiCorp submits that the security controls work must be completed to determine what categorizations are possible and needed. PacifiCorp has reviewed the existing controls and observes that many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
PEPCO	Disagree	We suggest the following:

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		BES Subsystem - A group of one or more BES Facilities (i.e. BES Generation Subsystem, BES Transmission Subsystem, and/or BES Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.
NEI	Disagree	A) Simplify to state "A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) B) Need to define what constitutes a "group" C) Doesn't aid Entities in identifying what needs to be protected, and, where assets are owned by more than one entity, how do the scenarios translate to subsystems or facilities, or the protection methodologies required? D) Defining groups of BES facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it may vary significantly with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Summary Consideration:

Organization	Yes or No	Question 1.d. Comment (Response page 8)
Progress Energy	Disagree	Remove "shared element or" from definition since these CIP standards are only intended to improve protections around cyber security assets.
EPSA	Agree	EPSA generally supports the definition and use of Generation Subsystem. However, the SDT is encouraged to formally define "shared element" and "shared Cyber System." The use of shared in this definition does not specify physical, ownership or other intangibles that could constitute shared elements.
GSOC/OPC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including generation units” is unclear; if the intent is to say that “multiple generation units whose combined output etc” must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Hayden	Disagree	1. Change the first line to read "Generation plants, or generation units including Facilities required to connect them to the Bulk Electric System (BES), singularly or in..." This is to emphasize that the focus is on the BES and not on distribution systems.
SDGE	Disagree	We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: Generation plants or generation units, including the Facilities required to connect them to a transmission system.
APPA	Disagree	APPA Task Force Comments: See Comment for BES Subsystem. No comments on the SDT’s proposed definition if this approach is adopted.
Consumers	Disagree	There is no need to introduce this term. The NERC Guide already addresses this as “common mode” failure. See Section 13.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
NPCC	Disagree	Definitions should not include impact. Recommend the following definition - Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination.
MPPA	Agree	
Central Lincoln	Disagree	Don't see how the part past the final comma adds anything to the definition. Who decides whether each unit within the plant or the plant itself constitutes a subsystem and how? Although the guidance document states the level of granularity is up to the registered entity, the draft standard does not make this statement. We think the SDT meant generation subsystems to be a subset of the BES subsystems. The proposed definition does not state this, though, and roof top photovoltaic systems may unintentionally be included.
NERC	Disagree	1. The concept of "misuse" needs to be captured along side of the current concepts of availability, degradation and compromise; 2. The definitions and application of Transmission Subsystems and Generator Subsystems provides the opportunity for artificial behavior in categorizing impact levels. The categorization process could drive entities to de-couple cyber systems that support multiple assets within an existing subsystem in order to classify them as different subsystems, each with a corresponding lower impact level. Those actions can result in additional security weaknesses and possibly impact the reliable operations of the subsystem.
Dominion	Disagree	See comments to 1.b. In addition to those comments, Dominion suggests that if the term "Element" is used in the context of cyber security, then greater specificity be added to the definition of "Element."
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	This definition needs to be tied back to the BES registration requirements. The Definition should be modified to reflect that the elements are components of a BES facility. The word "BES" needs to be inserted as follows: BES Generation Subsystems BES Generation plants The words "of a BES" need to be inserted after "generation units". The last part of the sentence should be deleted as it does not add to the definition by implying that a loss of generation facility output could compromise its control. The words "including generation units whose combined output could become

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		unavailable due to loss or compromise of a shared element or shared Cyber System" should be deleted. The SDT should carefully evaluate the need to use this term. It creates an overlap with the new definition proposed by the SDT for BES Subsystems. The language in this standard could easily rely on BES systems when it intends to refer to generation facilities and then restrict Generation Subsystems to aggregate or singular generating units. That would fit better with Attachment 1.
Dyonyx	Disagree	The use of the terms "Facility" in the context of this CIP Reliability Standard in defining "Generation Subsystem" is complicated by the convoluted nature of the definition of the former terms ("Facility" and "Element") in the current NERC Glossary of Terms and extends the confusion accordingly. Also, will there be any mention of the need to consider units and facilities less than 20 MW and 75 MW respectively?
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	Generation plants, comprised of single generation units or in combinations of units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.
Oregon PUC		No comment
NB Power Gen	Disagree	Perhaps the definition would be clearer if there were two sentences. The phrase "...including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System." could be a separate statement within the definition. E.g., A Generation Subsystem also includes generating units or facilities having any shared element or cyber system whose loss or compromise may cause the combined output to become unavailable.
Manitoba 1	Agree	
Portland GE	Disagree	We propose: "Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination." Delete everything after "combination" in the third line.
PSEG	Disagree	Comment #1: Concerned about the use throughout these documents of the words Facilities, Elements, and subsystem. These do not appear in the glossary and in some cases appear confusing and potentially conflict with those interpretations used in other NERC standards: TPL, FAC, EOP, etc. Comment #2: There is no need to introduce this term. The NERC Guide already addresses this as "common mode" failure.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		In addition, Wisconsin Electric Power Company has the following comments: The text "… including the Facilities required to connect them to a transmission system …" may cause an entity to secure or enclose all generating facilities' transformers and switch yards, which may not be the intent of the standard. We will need further clarity for " … shared Cyber System …". For example, if each generation plant distributed control system has its own network and can operate when disconnected from the common and high level network, is the loss or compromise of these shared elements have to be considered?
Idaho Power	Disagree	Need to define element. It would be helpful to provide some examples of what might constitute a shared element.
SOCO	Disagree	This definition extends beyond the scope identified in the purpose as stated on page 4 of the Standard. The Standard is intended to categorize "BES Cyber Systems" and this definition appears to extend into the area of "physical systems". The use of the word "element" would indicate that a manually controlled conveyor, or even a rail system, providing fuel to multiple generation units would be subject to categorization. The loss of these "elements" could impact plant operations over an extended failure period, but may not be subject to a cyber event. The words "Generation plants" should be removed. It adds no additional value, "Generation Units" and their facilities identify a clearer subsystem. The word "Facilities" should be replaced with "supporting subsystems" to indicate equipment vs. an entire plant site. Suggested definition Generation units including the supporting subsystems required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared Cyber System.
DTE	Agree	
AEP	Disagree	Defining groups of generation facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Disagree	The use of the terms "Facility" in the context of this CIP Reliability Standard in defining "Generation Subsystem" is complicated by the convoluted nature of the definition of the former terms ("Facility" and "Element") in the current NERC Glossary of Terms and extends the confusion accordingly.
Calpine	Agree	

Organization	Yes or No	Question 1.d. Comment (Response page 8)
NS&T	Disagree	See previous comment on BES Subsystem. The common "shared Cyber System" criterion could compel the process of identifying "Generation Subsystems" to be iterative and, as a result, inordinately time-consuming. We urge the SDT to strive for a simpler and more concise definition for the sake of consistency across multiple Entities and Regions, and also to allow finite resources to be applied to the most important task = improving cyber security. We believe, in addition, this would serve the goal of being able to perform audits in an efficient and consistent manner across the various Regions.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently. Also, if used should only apply to generation over 25 MW nameplate per GO/GOP criteria.
E ON	Disagree	Because nearly all generating units are tied into SCADA/EM systems the definition appears to allow for any combination of a registered entity's generating units from all units to any number/combination of less than all units. In order to comply an entity would need to classify every conceivable combination, or remove units from SCADA/EM systems. It is unclear whether the term "Facilities" refers to the Facilities identified in FAC-008/009.
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	On November 16, 2009 NERC issued the "Final Report from the Ad Hoc Group for Generator Requirements at the Transmission Interface" defining what is considered part of 'generation' and what's part of 'transmission' in different interface scenarios. This definition does not embrace the granularity of that guidance.
CenterPoint	Disagree	Disagree – See comments on 1.a, 1.c, and 8. However, some of the concepts in this proposed definition, such as the concept of shared elements or cyber systems, could possibly be added to CIP-002-2 - R1.2.3 for additional clarification.
LCRA	Agree	
FRCC	Disagree	See comment to question 1.a.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility and element within the proposed definitions.
ConEd	Disagree	Add "One or More" to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
EEI	Disagree	The current definition is confusing. The phrase "singularly or in combination," brings significant uncertainty as to the intended objective. We suggest:

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		Generation Subsystem — Generation plants, protection systems, or generation units including the Facilities required to connect them to a transmission system, generation units whose combined output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.
O&R	Disagree	Comments: Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
Alliant	Disagree	We believe the definition needs to be reworded as noted below for clarity: "BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss of compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem." Please clarify "shared." The terms "generation plant", "generation unit", and "transmission system" need to be defined in the NERC Glossary of terms.
Ameren	Disagree	This definition is too vague and confusing. The phrase “singularly or in combination” brings significant uncertainty as to the intended objective. What is the definition of “shared element”? This needs to be a defined term.
Black Hills	Disagree	Need to identify that this is a subset of the BES Subsystem definition. Might be better to stop the definition after the word 'combination'. Concern that the subsequent qualifiers ("whose combined output") could make separate generators (too small to even be registered with NERC) to be affected by this definition because of a "shared element or shared Cyber System". "element" should be "Element".
TNMP	Disagree	TNMP sees this definition as satisfactory. It accomplishes the intention of defining a Generation system without being overly broad and is properly constrained even with the inclusion of “Facilities required to connect”. When one looks at the NERC definition of Facilities it is clear that it is limited to discrete elements (e.g. lines, transformers) not an entire switching station. The connection would be to a Transmission Subsystem, thus, the R2 requirement of the proposed standard.
NVEnergy	Disagree	Some clarity is warranted with this definition. For instance, what constitutes the “transmission system” in the context above? We would assume that this is the point of connection of the Generator Step Up transformer to the high voltage bus, but this could be interpreted to include an entire transmission switching station if not clarified otherwise. This definition is overly broad for a “subsystem”. The description here more accurately describes an entire Generation System. We believe there needs to be some constraint in this definition on a locational basis within the BES. Suggested language: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination if their combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.”

Organization	Yes or No	Question 1.d. Comment (Response page 8)
Empire	Disagree	Optional definition: A group of one or more generation units controlled and/or monitored by a common BES Cyber System.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Disagree with Cyber System Definition in 1a.
SCEG	Disagree	This definition could, in the extreme interpretation, be problematic because of the phrase "or shared Cyber System." If that phrase is struck from the end of the sentence, the definition is fine. Strictly interpreted by the definition, one physical access control system that controls access to the facilities at all of the power plants would mean that they become one generation subsystem. In other words, all of the generation plants/units attached to any BES cyber system would become a single Generation Subsystem. This seems to contradict wording in the proposed standard that contemplates more than one subsystem connected to a single cyber system. It says in R3.2: "Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."
Exelon	Disagree	Exelon has concerns that the proposed definition may be open ended and subject to vastly differing interpretations (e.g. singularly or in combination) and suggest the following revisions: Generation Subsystem — Generation plants, or generation units at a common site including the Facilities required to connect them to a transmission system, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared BES Cyber System.
BPA Trans	Disagree	We propose: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination.” Delete everything after “combination” in the third line.
HQT	Disagree	Definitions should not include impact Recommend the following definition - Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination.
Allegheny Supply	Agree	Generation Subsystem – the term “shared element” in the “Generation Subsystem” definition is too broad and needs clarification. This term is critical to the definition of a “Generation Subsystem”. (e.g. This definition could be interpreted to mean that all generation is a single “Generation Subsystem” because is has the transmission system as a shared element.)
KCPL	Disagree	No, this definition should limit itself to the generation facility itself. The terms, “shared element or shared Cyber System” are too vague as to what that represents and, again, makes this definition conditional. The CIP standard should identify

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		the facilities to be included for evaluation (as this is attempting to do) and allow the process for determining the impact a facility or facilities has on the BES to drive the appropriate level of cyber protection.
Connectiv Energy	Agree	One concern is that "Shared Element…" would be defined to include a Transmission Owner's asset (farther up the line from a single plant connection) to which generating units from more than a single GO are attached? In this case would NERC look to aggregate generation from more than a single GO which singularly might not be part of the BES but due to their "Subsystem" connection could force them into the BES due to the combined total generation? This would not be desirable.
MidAmerican	Disagree	See MidAmerican's summary comments in question 13 and comments on BES Subsystem above in 1.c. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the "iron" (generating unit) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase "singularly or in combination." If the definition is needed, it should refer to the distributed control systems for BES generating units in scope. New NERC Glossary definitions must carefully consider for impacts to other NERC standards.
CPG	Disagree	This definition of Generation Subsystem should clearly identify that it includes all equipment from the point of interconnection to the generating unit(s). Facilities required to connect them to the transmission system could mean a bus, a transformer, a switch, a breaker, and so forth. It is too broad.
Santee Cooper	Agree	
OGE	Disagree	• Provide clarity on your definition of a "shared element" and "shared Cyber System". Fuel source? Water Source? Train Tracks? • Adequate detail is required to avoid incorrect interpretations by all parties. • What is the purpose of the last part of the definition, "…including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System…"? It seems as though that is a subset of what has already been described by the first part of the definition. • What level of output from a single or combination of unit that would affect the Bulk Electric System? • OPTION: A group of one or more generation units controlled or monitored by a common BES Cyber System. Once clarity is achieved for what is meant by "common BES Cyber Systems".
PPL Supply	Disagree	Comments: Agree with EEI comment that the definition can be unclear. However, removing "singularly or in combination," as proposed by EEI does not improve the clarity. In addition EEI's proposed definition adds "protection systems", which does not seem to be appropriate for the definition of generation sub-system. Protection systems should be considered and evaluated as Cyber Systems.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		We propose the following definition: Generation plants, or generation units (singularly or in combination), including the Facilities required to connect them to a transmission system, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.
St. George	Agree	
NGRID	Disagree	National Grid believes that the definition should not include impact and propose the following definition “Generation plants or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination”.
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to a Generation Subsystem(s) connected at 100kV or greater. Many entities are not vertically integrated where they do not own the generator and transmission elements collectively. As written, a GO may be responsible for TO Facilities. A GO may not have the understanding of the limitations and capabilities of a TO Facility. Please clarify. As written please clarify what a “shared element” is since “Element” is not capitalized as in question 1.e. Recommend rewriting to include “shared cyber element”, this will clearly define the intent of the definition. Refer to question 1.a. concerning a shared “Cyber System”. As written if there is no “shared element” then the stand alone generator connected at 100kV and above is not a Generation Subsystem. Please clarify what a “shared element” refers to. Is this a cyber element that is common to two generators or could this be a non cyber physical element? Recommend that physical elements (non cyber) not be covered by CIP Standards. Please clarify if the definition is attempting to identify Generation plants/units including Facilities and their components (breakers, RTUs, unit control systems) or the cyber protection systems that guard against cyber attacks. Recommend that Generation Subsystem definition be rewritten to clearly define what a Generation Subsystem is. Recommend the definition to read: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination”. The remaining proposed SDT definition should be added to Attachment 1 since the intent seems to be a sub component of what the intent of the definition actually is trying to state.
FE	Disagree	The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System".
TECO	Disagree	We support EEI’s comment and suggest the following changes to the proposed definition. Generation Subsystem — Bulk Electric System Generation plants, protection systems, or generation units including the Facilities required to connect them to the Transmission Subsystem, generation units whose combined output could

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		become unavailable due to loss, compromise, or significant degradation of shared BES Cyber System.
CECD	Disagree	The definition should be modified as follows: Generation plants or generation units, including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System.
MRO	Disagree	We feel the definition is ambiguous as written, and propose the following reworded definition for clarity: BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss or compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem. We also would like a clarification of “shared” as we had disagreement just within our MRO NSRS group on what this term implied. Regardless, the terms “generation plant”, “generation unit”, and “transmission system” should be defined in the NERC Glossary of Terms.
GTC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including generation units” is unclear; if the intent is to say that “multiple generation units whose combined output etc” must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Xcel	Disagree	We feel the definition is ambiguous as written, and propose the following reworded definition for clarity: BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss or compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem. We also would like a clarification of the term “shared”. The terms “generation plant”, “generation unit”, and “transmission system” should be defined in the NERC Glossary of Terms. The Standard needs to include a clarification where remote generation assets controlled from one plant can also be treated as multiple units at a plant facility. I.e.: Plant site has four units, no shared connectivity, same thing for remote plant/unit if the controls are independent from the controlling plant controls.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
BGE	Disagree	The last term of item 1.d. should be “BES Cyber System”, not “Cyber System”, since we recommended the removal of the definition of “Cyber System”. The term, “shared element” is vague and may include items unrelated to cyber security. We recommend that the term “shared element” be omitted. We recommend the following definition: Generation Subsystem — Generation plants, or generation units, including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System. Communication networks and data communication links between discrete BES cyber systems need not be considered as a “shared cyber systems” in the determination of facilities that constitute BES Subsystem. Even with this modification, we are concerned that the definition is overbroad in that there is no limit to combining disparate systems and considering them a single subsystem.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective.
FMPA	Disagree	As discussed above, there is no need for adding the concept of Subsystems. Also, FMPA does not see a reason to define Generation, Transmission and Control Center Subsystems separately, which can introduce opportunities for confusion and for the definitions to conflict with each other. FMPA recommends eliminating the concept of subsystems. Failing that, we would recommend eliminating the sub-sub-systems of Generation, Transmission and Control Center subsystem. Failing that, if the SDT insists on retaining this concept, the definition is confusing and complicated and could be greatly simplified by: “Generation and associated Facilities that share a common Cyber System” We fail to see why sharing a common Element is important to this standard. If it is a common mode failure that the SDT is concerned about, that will already be captured in the criteria for any Cyber System that controls that shared Element. The purpose of the standard is to determine which Cyber Systems’ cyber security to regulate, so, if the SDT decides to keep the unnecessary concept of Subsystems, they should not be determined by shared elements, but by shared Cyber Systems. Again, the NERC Glossary of Terms should be used when appropriate and the word “Element” should be capitalized (for clarity, we should never use a non-capitalized word that is in the NERC Glossary); however in this case the more appropriate term should be “Facility” since it is part of the BES. Note also that we should be consistent with using BES as an adjective. If the SDT chooses to retain the unnecessary

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		concept of Subsystems, then the SDT ought to either rename this “BES Generation Subsystem”, or rename “BES Subsystem” as just “Subsystem”.
Duke	Disagree	This definition should be revised to clarify that a control room for a multiple unit site would be part of the site, and would not be considered a Control Center. Suggested wording: Generation Subsystem – Generation plants, or generation units including the facilities up to the point of interconnection with the transmission system.
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including generation units” is unclear; if the intent is to say that “multiple generation units whose combined output etc” must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
IESO	Agree	
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.d. Comment (Response page 8)</th></tr>
<tr><td></td><td></td><td>appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Generation Subsystem — Generation plants or units as identified in the Registration Criteria including the Facilities required to connect them to a transmission system, BES protection systems, and generation units whose combined</td></tr>
</table>

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.
IMPA	Disagree	This definition is not very clear on how a generation plant needs to be classified if it has more than one generating unit. It is not clear how to classify multiple units that are connected into a ring bus. In this scenario, can a Generation Subsystem be one plant with multiple units each connected to a ring bus via individual generator step-up transformers? The meaning of "shared" needs to be defined. Generating Units may share elements in a ring bus in a substation, but the loss of one shared element may make only one generating unit unavailable and not the other generating units.
PacifiCorp	Disagree	See PacifiCorp's summary comments in question 13 and comments on BES Subsystem above in 1.c. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the "iron" (generating unit) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase "singularly or in combination." If the definition is needed, it should refer to the distributed control systems for BES generating units in scope.
PEPCO	Disagree	The current definition is confusing. The phrase -singularly or in combination-, brings significant uncertainty as to the intended objective. We suggest the following: BES Generation Subsystem - Generation plants or generation units including the BES Facilities required to connect them to a transmission system whose output could become unavailable due to loss or compromise of a BES Element or BES Cyber System.
NEI	Disagree	A) The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System". B) On November 16, 2009 NERC issued the "Final Report from the Ad Hoc Group for Generator Requirements at the Transmission Interface" defining what is considered part of 'generation' and what's part of 'transmission' in different interface scenarios. This definition does not embrace the granularity of that guidance. C) Clarification is sought on what exactly the phrase "including the Facilities required to connect them to a transmission system" entails. We believe this means transformers and transformer support systems, and want to ensure that this isn't construed as the generating station Control Room. D) Suggest the addition of "as defined by the local interface agreement" after "transmission system" to ensure the boundaries are clear to the Generator. E) Defining groups of generation facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		may vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Summary Consideration:

Organization	Yes or No	Question 1.e. Comment (Response page 9)
Progress Energy	Disagree	Remove "shared element or" from definition since these CIP standards are only intended to improve protections around cyber security assets.
GSOC/OPC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including transmission lines or busses” is unclear; if the intent is to say that “multiple transmission lines or busses whose combined output etc” must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term “output” with “capacity”. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Hayden	Disagree	Need to emphasize connection to and support of the Bulk Electric System. Adding some sort of focus on the BES in this definition is needed.
SDGE		We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: Transmission substations, transmission busses, or transmission lines including the Facilities required to interconnect them.
APPA	Disagree	APPA Task Force Comments: See Comment for BES Subsystem. No comments on the SDT’s proposed definition if this approach is adopted.
Consumers	Disagree	Although probably not the intent, this definition seems to limit the subsystem to only those assets “… whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.” In addition, it should be noted that although a ‘shared cyber system’ may cause the loss of several BES elements, there may not be an impact to system reliability. See Section 13.
NPCC	Disagree	Definitions should not include impact Recommend the following definition - Transmission substations, transmission busses, or transmission lines including the

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination.
MPPA	Agree	
Central Lincoln	Disagree	Again we fail to see how the part past the final comma adds any elements or clarity to the part that precedes it. And how does one determine whether the individual busses within a substation constitute individual subsystems, or whether the entire substation constitutes a subsystem? Although the guidance document states the level of granularity is up to the registered entity, the draft standard does not make this statement. As above, the definition should be modified to make it clear that transmission subsystems are a subset of the BES systems.
NERC	Disagree	1. The concept of “misuse” needs to be captured along side of the current concepts of availability, degradation and compromise; 2. The definitions and application of Transmission Subsystems and Generator Subsystems provides the opportunity for artificial behavior in categorizing impact levels. The categorization process could drive entities to de-couple cyber systems that support multiple assets within an existing subsystem in order to classify them as different subsystems, each with a corresponding lower impact level. Those actions can result in additional security weaknesses and possibly impact the reliable operations of the subsystem.
Dominion	Disagree	See comments to 1.b. and 1.d. above.
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	The definition needs to be tied back to the BES registration requirements similarly to the Definition for Generation Subsystems. This definition has the same duality problem as Generation Subsystems.
Dyonyx	Disagree	The use of the terms “Facility” and “Element” in the context of this CIP Reliability Standard in defining “Transmission Subsystem” is complicated by the convoluted nature of the definition of the former terms (“Facility” and “Element”) in the current NERC Glossary of Terms and extends the confusion accordingly.
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	Does not draw a "bright line" around Generation switchyards as to the EXACT point it becomes transmissions

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		responsibility.
Oregon PUC		The term "compromise of …" is too broad and leaves too much room for auditor and enforcement interpretation.
Manitoba 1	Agree	
Portland GE	Disagree	We propose "Transmission substations, transmission busses or transmission lines including the Facilities required to connect them to Elements, singularly or in combination." Delete everything after "combination" in third line.
PSEG	Disagree	Comment #1: We believe that the proposed definition could be interpreted to two different ways. a. The definition is attempting to identify the Facilities in the substation (examples: Breakers, switches, tap changers and real-time data) controlled through a BES Cyber System. b. The definition is attempting to identify the BES Cyber System which controls the breakers, switches, tap changers and real-time data in a substation. The difference between the two interpretation is that one will contain a list of Facilities (Breakers, switches, tap changes) while the other contains a list of electronic devices control Facilities. It is our understanding that the first interpretation is the proper understanding and makes the following suggestion to the definition. Is made up of devices that are able to change state (open, close) change voltage levels (tap changers, cap banks) and collect real-time data (CT, VT, PMUs) and contained with a BES Cyber System. (NOTE: See our suggested definition of a BES Cyber System) Two Examples: 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. The goal of our suggested definition is to make it clear that a Transmission Subsystem can be made up of all, portion of or multiple substations based on an entities ESP configuration at the substation level. Comment #2: We believe that there is inconsistent use of terms compared to other NERC standards.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.
Idaho Power	Disagree	Need to define element. It would be helpful to provide some examples of what might constitute a shared element.
SOCO	Agree	It should be noted that although the 'shared cyber system' may cause the loss of several BES elements, there may not be an impact to system reliability.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
DTE	Agree	
AEP	Disagree	Defining groups of transmission facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Disagree	The use of the terms “Facility” and “Element” in the context of this CIP Reliability Standard in defining “Transmission Subsystem” is complicated by the convoluted nature of the definition of the former terms (“Facility” and “Element”) in the current NERC Glossary of Terms and extends the confusion accordingly.
Calpine	Agree	
NS&T	Disagree	See previous comment.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	Again, given the pervasiveness of SCADA/EM system connectivity, the definition establishes a nearly unlimited number of combinations, i.e. transmission subsystems.
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	What’s an “Element” (one time capitalized, another not) – definition provides no clarity; counterproductive.
CenterPoint	Disagree	Disagree – See comments on 1.a, 1.c, 1.d, and 8. However, some of the concepts in this proposed definition could possibly be added to CIP-002-2 - R1.2.2 for additional clarification.
LCRA	Agree	
FRCC	Disagree	See comment to question 1.a.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility and element within the proposed definitions.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
ConEd	Disagree	Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
EEI	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective. We suggest: Transmission Subsystem — Transmission substations, protection systems, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.
O&R	Disagree	Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
Alliant	Disagree	We believe the definition needs to be revised as noted below: "BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem." Please clarify the definition of "shared." The terms "transmission substation" and "transmission bus" need to be added to the NERC Glossary of Terms, and "transmission lines" should be replaced with "Transmission Lines."
Ameren	Disagree	The words "whose combined output" should be removed and replaced with "that". A transmission system does not output anything. The definitions of Generation Subsystem and Transmission Subsystem BOTH include "Facilities required to connect" generators to Transmission. Since FERC, RRO and virtually all state Commissions have the generator owning the GSU, ONLY the Generation Subsystem definition should only be included in "Facilities required to connect" generators to Transmission. What is the definition of “shared element”? This needs to be a defined term.
Black Hills	Disagree	Need to identify that this is a subset of the BES Subsystem definition. Might be better to stop the definition after the word 'combination'. What is the "combined output" of transmission lines? (Net MVA capability?). The last use of "element" should be "Element".
TNMP	Disagree	The phrase “whose combined output could become unavailable” is not clearly applicable to all Transmission Subsystems. A Transmission substation should always have a net of all inputs and outputs to be zero. None of the criteria in CIP-002 Attachment 1 look at the total output of a Transmission Subsystem to evaluate the Transmission Subsystem Impact rating. The definition should be rewritten to clear up any confusion.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
NVEnergy	Disagree	With this definition, it is unclear what level of aggregation of the various busses, lines, stations, etc. is allowed or expected. The definition uses defined NERC terms as “Facilities” and “Elements”, yet the degree of granularity seems to be inconsistent (for example, how can a Transmission substation include Facilities that are required to connect with an Element). Note that much of the confusion in this definition is a result of our lack of understanding of the difference between the NERC-defined terms used here. Beyond that, however, the use of the phrase beginning with “including transmission lines…” infers that the definition is not limited to those collections of elements whose output could be subject to common mode loss, and therefore includes other collections of elements whose groupings are not well-defined.
MWDSC	Disagree	Appears to suffer from circular logic - by linking a substation to a cyber system, doesn't it force a conclusion that it has a medium or high impact?? Transmission Subsystems may become unavailable for many reasons, but loss of one substation or element may not affect an interconnected system. See following comments on impact levels.
Empire	Disagree	Alternative suggestion: A group of one or more transmission facilities operated at 200 kv and above that are controlled and monitored by a common BES Cyber System.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	A better definition of "Facilities" and what is included.
SCEG	Disagree	Strike "or shared Cyber System" per the comments in 1.d, or recommend changes to the language in R3.2. The definition is at odds with the proposed standard.
Exelon	Disagree	Exelon has concerns that the proposed definition may be open ended and subject to vastly differing interpretations (e.g. singularly or in combination) and suggest the following revisions: Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared BES Cyber System.
BPA Trans	Disagree	We propose “Transmission substations, transmission busses or transmission lines including the Facilities required to connect them to Elements, singularly or in combination.” Delete everything after “combination” in third line.
HQT	Disagree	Definitions should not include impact Recommend the following definition - Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination.
Allegheny Supply	Agree	

Organization	Yes or No	Question 1.e. Comment (Response page 9)
KCPL	Disagree	No, this definition should limit itself to the transmission facility itself. The terms, “shared element or shared Cyber System” are too vague as to what that represents and, again, makes this definition conditional. The CIP standard should identify the facilities to be included for evaluation (as this is attempting to do) and allow the process for determining the impact a facility or facilities has on the BES to drive the appropriate level of cyber protection.
Connectiv Energy	Agree	Similar to the answer to 1d, one concern is that “Shared Element…” would be defined to include a Transmission Owner’s asset (farther up the line from a single plant connection) to which generating units from more than a single GO are attached? In this case would NERC look to aggregate generation from more than a single GO which singularly might not be part of the BES but due to their “Subsystem” connection could force them into the BES due to the combined total generation? This would not be desirable.
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13 and comments on BES Subsystem above in 1.c. and 1.d. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the “iron” (substation) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase “singularly or in combination” and in the use of NERC Glossary terms “Element” and “Facility.” As currently written, the definition’s scope could be a single circuit breaker up to and including all electrical facilities within a balancing authority area. Such a broad and vague term may cause difficulties implementing, auditing and proving compliance. If the definition is needed, MidAmerican proposes that its scope be limited to transmission substations and Special Protection Systems.
CPG	Disagree	This definition should clearly demarcate from the point of interconnection to the distribution system.
Santee Cooper	Agree	
OGE	Disagree	• Please provide a definition of "shared element" for electric transmission and other entities. • OG&E requests clarification on the “transmission subsystem” definition; Is there an expectation that every line segment be uniquely identified and classified? • OPTION: A group of one or more transmission Facilities controlled or monitored by a common BES Cyber System. Once clarity is achieved for what is meant by “common BES Cyber Systems”.
Oncor	Disagree	BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem.
PPL Supply	Disagree	Agree with EEI comments.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
St. George	Agree	
NGRID	Disagree	National Grid believes that the definition should not include impact and propose the following definition “Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination”.
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to a Transmission Subsystem(s) connected at 100kV or greater. Refer to question 1.a. concerning a shared “Cyber System”. As written if there is no “shared element” then the stand alone Transmission Subsystem connected at 100kV and above is not a Transmission Subsystem. Please clarify what a “shared element” refers to. Is this a cyber element that is common to two generators or could this be a non cyber physical element? Recommend that physical elements (non cyber) not be covered by CIP Standards.
FE	Disagree	The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System".
TECO	Disagree	We support EEI’s comments and suggest the following changes to the definition. Transmission Subsystem — Bulk Electric System Transmission substations, protection systems, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss, compromise, or significant degradation of a shared BES Cyber System.
CECD	Disagree	The definition should be modified as follows: Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System.
MRO	Disagree	We feel the definition is ambiguous as written, and would propose the following reworded definition for clarity: BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem. We also would like a clarification of “shared” as we had disagreement just within our MRO NSRS group on what this term implied. Regardless, the terms “transmission substation” and “transmission bus” should be defined in the NERC Glossary of

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		Terms, and “transmission lines” should be replaced with “Transmission Lines” to remove further ambiguity.
GTC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including transmission lines or busses” is unclear; if the intent is to say that “multiple transmission lines or busses whose combined output etc” must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term “output” with “capacity”. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Xcel	Disagree	We feel the definition is ambiguous as written, and would propose the following reworded definition for clarity: BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem. We also would like a clarification of the term “shared”. The terms “transmission substation” and “transmission bus” should be defined in the NERC Glossary of Terms, and “transmission lines” should be replaced with “Transmission Lines” to remove further ambiguity
BGE	Disagree	Change “Cyber System” to “BES Cyber System” The term, “shared element” is vague and may include items unrelated to cyber security. We recommend that the term “shared element” be omitted. We recommend the following definition. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System. Communication networks and data communication links between discrete BES cyber systems need not be considered as a “shared cyber systems” in the determination of facilities that constitute BES Subsystem. Even with this modification, we are concerned that the definition is overbroad in that there is no limit to combining disparate systems and considering them a single subsystem.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective.
FMPA	Disagree	See FMPA’s comments to 1.d.
Duke	Disagree	This definition should be revised to remove ambiguity. Suggested wording: Transmission Subsystem – Transmission substations or Transmission lines.
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including transmission lines or busses” is unclear; if the intent is to say that “multiple transmission lines or busses whose combined output etc” must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term “output” with “capacity”. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
IESO	Agree	
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	ATC believes that the proposed definition could be interpreted in two different ways. 1. The definition is attempting to identify the Elements in the substation (examples: Breakers, switches, tap changers and real-time data) controlled through a BES Cyber System. 2. The definition is attempting to identify the BES Cyber System which controls the breakers, switches, tap changers and real-time data in a substation. The difference between the two interpretations is that one will contain a list of Elements (Breakers, switches, tap

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.e. Comment (Response page 9)</th></tr>
<tr><td></td><td></td><td>changes) while the other contains a list of electronic devices that control Elements.
It is our understanding that the first interpretation is the proper understanding and we make the following suggestion:
“Is made up of devices that are able to change state (open, close) change voltage levels (tap changers, cap banks) or collect real-time data (CT, VT, PMUs) and contained within a BES Cyber System.”
(NOTE: See our suggested definition of a BES Cyber System)
Two Examples:
1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystems.
2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem.
The goal of our definition is to make it clear that a Transmission Subsystem can be made up of all, portion of or multiple substations based on an entities ESP configuration of its BES Cyber System.</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.e. Comment (Response page 9)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Puget Sound Energy requests clarity of the term Transmission.
Transmission Subsystem- Bulk Electric Transmission Facilities including substations, protection systems, transmission busses, or transmission lines and equipment required to connect them to Elements, that could become unavailable due to loss or compromise of a shared BES Cyber System.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The definition is not clear and very confusing. IMPA recommends clarifying what exactly is meant by the terms “singularly or in combination” in the definition of the Transmission Subsystem. In addition, it would help with the clarity of the definition if transmission busses and transmission substation were defined in the NERC glossary. The term transmission lines should be changed to reference the NERC glossary (Transmission Lines).
The meaning of “shared” needs to be defined.</td></tr>
<tr><td>PacifiCorp</td><td>Disagree</td><td>See PacifiCorp’s summary comments in question 13 and comments on BES Subsystem above in 1.c. and 1.d.
The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the “iron” (substation) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset.</td></tr>
</table>

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		The CIP-002-4 definition, if needed, is confusing, especially the phrase “singularly or in combination.” The definition as currently written should specify more clearly the scope of the term. As currently written, the definition could be a single circuit breaker to all electrical facilities within a balancing authority area. Such a broad and vague term may cause difficulty for auditing as well as for proving compliance. If the definition is needed, PacifiCorp proposes that is scope be limited to transmission substations, protection systems, transmission busses or transmission lines.
PEPCO	Disagree	The current definition is confusing. The phrase - singularly or in combination - brings significant uncertainty as to the intended objective. In addition while the transmission subsystem consists of the various elements described in addition to other elements such as transformers, we believe that the cyber security standards if using the Big Iron method should classify at the substation level (i.e. the bus(es), line(s), or transformer(s) help determine the impact level of the substation). The phrase - including transmission lines or buses whose combined output could become unavailable - is confusing as transmission subsystems usually are not referred to as having output like generators. Rather than output, transmission subsystems have throughput or capability/capacity. We suggest the following: BES Transmission Subsystem — BES Transmission substations made up of BES Elements and BES Facilities (e.g. BES transmission busses, BES transmission lines, and/or BES transformers) which could become unavailable due to the loss or compromise of a BES Element or BES Cyber System.
NEI	Disagree	A) Revise to “Transmission substations and transmission lines.” B) If A) is not followed, the term “shared element” is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared “Cyber System” to shared “BES Cyber System”. C) Defining groups of transmission facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

Summary Consideration:

Organization	Yes or No	Question 1.f. Comment (Response page 10)
Progress Energy	Disagree	The definition of Control Center needs to specify that control rooms in power plants or transmission substations are NOT included in the definition of Control Centers.
Dynegy	Disagree	1. The term “BES assets” is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: “A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…” 2. In the third bullet, the terms “and asset management” need to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term “BPS” should be replaced by “BES”.
GSOC/OPC	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity. With respect to the first bullet of the definition, we suggest changing it to the following ”Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		systems; or automatic load-shedding systems” We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a control center. The phrase “capable of” is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term “Situational awareness”.
Hayden	Agree	
SDGE	Disagree	For clarification, we propose new wording for this definition as follows: A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations performed by a Control Center include, but are not limited to, one or more of the following: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems • Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BES) • Coordination of BES restoration activities.
APPA	Disagree	APPA Task Force Comments: Control Center The definition of Control Center needs clarification. There are primary and back-up Control Centers that have the assigned and contractual responsibility for the functions listed in the Control Center definition described in Version 4 that are performed by a Balancing Authority and Transmission Operator with Reliability Coordinator oversight. There are owners of distribution facilities who also own BES assets who have alarm monitoring and data collection capabilities for these facilities and assets but they do not and will not have remote supervisory control for BES assets. The facilities and BES assets of these owners who are merely monitoring and collecting information should not be required to have their facilities classified as Control Centers under the CIP standards. These owners have contracted with other entities to perform Control Center functions. A change to this proposed definition is needed to ensure that that an owner’s identification of alarm monitoring capability does not make the facility subject to the Control Center requirements. For this reason, the fourth bullet under the Control Center definition, “Alarm monitoring and processing” should be changed to

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		"Alarm processing".
Consumers	Disagree	Why the use of the term, Bulk Power System? Also, an equipment room containing a front-end processing unit which received data from multiple substations would perform the function listed in the second bullet and therefore qualify as a control center. At power plants, often the unit control room controls the generating unit (or multiple units) and also has supervisory reclosing capability of the generator high side breakers out in the plant switchyard. Therefore, this control room may be pulled into scope unintentionally. Also, we are reintroducing the term assets, without definition.
NPCC	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
MPPA	Agree	
Central Lincoln	Disagree	This definition might be interpreted to encompass every laptop computer or PDA outfitted with SCADA web client and/or alarm processing software. Suggest language that would clarify that fixed server locations are intended, and that remote clients are not. The term "BES asset" should also be defined. The first bullet implies all load-shedding systems, for example, are BES assets. The definition should be narrowed so that only those load-shedding systems that have a BES reliability impact are included. Perhaps "BES facility" should be used instead, in order to be consistent with the other proposed definitions.
NERC	Agree	
Dominion	Disagree	Dominion disagrees with the definition of "Control Center." Under the current definition, any one attribute, such as displaying system status or having a space dedicated to coordination of restoration, could qualify as a "Control Center." The definition is too broad and should be modified to emphasize that a "Control Center" should have the capability for: 1) data display; and 2) system control. Also, the listed examples should be illustrative as areas of consideration but not as specific qualifiers.
Encari	Disagree	"Control Center" is said to be capable of performing one or more of the functions for multiple (i.e., two or more) BES assets. The emphasis on "capable" invites confusion. A SCADA system may actually be used to control a single substation but be capable of controlling two substations if the SCADA system had the appropriate supporting network communication and configuration settings. The criteria for a control center should focus on its actual configuration and use, not its theoretical capability. The term "BES asset" is neither defined in the NERC Glossary nor in the Standard. For purposes of consistency, the term "BES Subsystem" should replace the term "BES asset" since both terms appear to have the same meaning within the

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		Standard. “BES Subsystem” is preferred since it is explicitly defined in the Standard. Additionally this definition of control center may lead to confusion due to the generic interpretation of "alarm monitoring and processing". Specifically this may include fire alarm systems, water suppression systems, physical security operation centers and any other centralized function with "alarm monitoring and processing". We recommend strengthening this definition to be more specific.
US ACE – NW	Disagree	Control center definition should not apply to multiple facilities that are located on the same property where data/controls are aggregated to a central control room. For example wind generators each have data collection and control systems in each tower and that data is fed to a central control room that is physically on the same property and commonly contained within the same physical security boundaries. Another example would be the many thermal and hydropower generating facilities that have multiple powerhouses on the same physical property with all controls centralized. So, the Control Center definition needs to only apply to those generating or transmission facilities that are not all located on the same physical property.
SCE	Agree	
USBR	Disagree	The definition implies a definition for BES assets which is not covered in the NERC Glossary. It should either define BES Assets or be modified to refer to BES Subsystems. As such the text following BES assets should be deleted. The third bullet item is redundant to the second bullet and should be deleted. The forth bullet is covered under the second bullet and should be deleted.
Dyonyx	Disagree	The definition of “Control Center” uses new terms that have not previously been defined which will add to the confusion in understanding the definition. Specifically, the term “BES Assets” is not defined. Why not use the term “BES Subsystem” or the proposed “BES Facility”? In terms of categorizing the “Impact” of a Control Center “Subsystem”, we believe it is important to realize that the “Impact” categorization of a Control Center is dependent upon the “Impact” of the underlying “Cyber Systems” contained within the Control Center. Accordingly, not all Control Centers are High Impact or even Medium Impact Subsystems. An iterative process will be required to properly establish the categorization of this particular BES Subsystem.
FMPP	Agree	
MISO	Disagree	The following changes need to be made to this definition: 1. The term “BES assets” is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: “A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…” 2. In the third bullet, the terms “and asset management” need to be removed. As currently written, the inclusion of this

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term “BPS” should be replaced by “BES”.
Westar	Disagree	Bullet one includes 'automatic load-shedding systems'. Underfrequency Load Shed programs, which I think would qualify as an automatic load-shedding system, are typically installed on the distribution system and not on the BES. Will this pull the pure Distribution Control Centers into the CIP requirements? Suggest eliminating the 'or automatic load-shedding systems'.
Green Country	Disagree	How does this affect previous definitions of "Control Room" and "Control Center". With respect to generation I believe the "Control Room" definition is appropriate. Control Room - A Control Room is typically located within the facility and operates control systems limited to controlling: 1. A single generation plant with one or more units. 2. A single transmission asset such as a transmission substation.
Oregon PUC		No comment
Manitoba 1	Agree	
Portland GE	Disagree	This definition has the potential for making substation control houses, or other facilities, where some type of control is exerted over more than one substation facility, fit within the definition of a “control center.” The NERC definition of Control Center should be consistent with what the Utility Industry normally uses to identify "Control Centers". We suggest a more concise definition as follows: Control Center – “A Facility from which System Operators (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) monitor and control transmission or generation Facilities in real time.” The definitions of these terms from NERC Glossary of Terms Used in Reliability Standards, updated April 20, 2009 were considered and used to develop the recommended definition: System Operator, Transmission Operator, Transmission, Generator Operator, Telemetering, Facility, and Element.
PSEG	Disagree	Comment #1: We mostly agree with the proposed definitions however, we question if NERC RCIS, NERC TLR; MISO Outage Scheduler, MISO Information System, OATI – would then fit this definition of a Control Center unintentionally. Comment #2: We would like to understand the intention of the substitution of the terms Bulk Power System (BPS) for Bulk Electric System (BES) in this definition.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.
Idaho Power	Agree	

Organization	Yes or No	Question 1.f. Comment (Response page 10)
SOCO	Disagree	While a specific definition of what constitutes a control center is necessary, a literal reading of the definition given would include far more facilities than are intended. For example, an equipment room containing a front-end processing unit which received data from multiple substations would perform the function listed in the second bullet and therefore qualify as a control center. While a good faith reading of the standard would not produce such results, good faith cannot be relied upon in all cases, so the definition must be tightened At power plants, often the unit control room controls the generating unit (or multiple units) and also has supervisory reclosing capability of the generator high side breakers out in the plant switchyard. Therefore, this control room may be pulled into scope unintentionally. The term “assets” should be identified – is this intended to mean “BES subsystem”? Suggested definition: A Control Center is capable of performing one or more of the functions listed below for geographically dispersed multiple sites (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: … This definition should be worded to delineate that it is not intended to included independently isolated generation units controlled from within the same control room or building. A control room for a two unit generation plant could interpreted to be included under the second bulleted item. Suggested insertion at bottom of definition: This is not intended to include control rooms at power plants intended exclusively for the control of generation units.
DTE	Agree	
AEP	Disagree	The open-ended nature and lack of clarity in this definition is concerning for the reasons described in the response to question 1a. This generally results from the approach of incorporating many technical functions into a single definition. As a result, there is a lack of clarity as to what is intended to be in scope and out of scope. For example, the descriptions could, perhaps unintentionally, even draw in plant control rooms or unit control rooms.
Edison Mission	Disagree	The definition of “Control Center” uses new terms that have not previously been defined which will add to the confusion in understanding the definition. Specifically, the term “BES Assets” is not defined. Why not use the term “BES Subsystem” or the proposed “BES Facility”? In terms of categorizing the “Impact” of a Control Center “Subsystem”, we believe it is important to realize that the “Impact” categorization of a Control Center is dependent upon the “Impact” of the underlying “Cyber Systems” contained within the Control Center. Accordingly, not all Control Centers are High Impact or even Medium Impact Subsystems. An iterative process will be required to properly establish the categorization of this particular BES Subsystem.
Calpine	Agree	

Organization	Yes or No	Question 1.f. Comment (Response page 10)
NS&T	Agree	
Flathead	Disagree	Existing definition of control center is sufficient. Currently control center does not include a dispatch center at a local distribution entity that may or may not be staffed 24-hours and does not function as a BA, TO, GO, or RC. The definition of control center should not be expanded with this standard. See current NERC Glossary re definition of a System Operator. System Operator An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.
E ON	Disagree	Bullet two would establish as a control center any location where BES reliability or operational data is being displayed. The same bullet would also qualify a Remote Transmitting Unit ("RTU") as a Control Center. The third and fourth bullet would establish nearly every substation control house, and any other facility housing control panels with alarm indicators and acknowledgement capability, as Control Centers. Clearly, the definition is far too encompassing. The drafting team would be well advised to pay particular attention to use of the conjunctives "and" and "or" in this standard.
Carthage		Again CWEP would like better clarification on BES. Please refer to 1C above.
WECC	Agree	Is the intent of this definition to bring in new entities that haven't previously been identified as having impact on the BES such as Market Control Systems?
Entergy	Disagree	This is not a definition – it's a list of examples of what might be that which is ill-defined.
CenterPoint	Disagree	Disagree – See comments on 1.a. However, some of the concepts in this proposed definition could possibly be added to CIP-002- 2 - R1.2.1 for additional clarification.
LCRA	Disagree	1. More explanation and definition is required as to why asset management is included. Asset management functions would normally not be essential for the operation and control of the BES Subsystem. Need to better define what specific asset management functions are included. 2. "BPS" is not defined. What does this mean?
NIPSCO	Disagree	We mostly agree with the proposed definition however, we question if the definition unintentionally expands the scope to include cyber systems that support real-time operations within the control center environment: RCIS, TLR, ARS, RC Outage Scheduler, RC Information System, OATI, etc.. Additionally, we would like to understand if it was the intention of the SDT to substitute the terms Bulk Power System (BPS) for Bulk Electric System (BES) in this definition only. Suggestion: Review the intended scope of the term control center and clarify the intent with revised or additional language.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
ConEd	Agree	
EEI	Disagree	Parts of the definition are too broad. For example, a literal interpretation of: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations" Could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. We suggest: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential used for real-time operations" • Bullet 4, "Alarm monitoring and processing", should be changed to read "BES alarm monitoring, processing and response.."
O&R	Agree	
Alliant	Disagree	We believe the bullet "Alarm monitoring and processing" should be removed, as this functionality should inherently be included as part of the other processes listed. In some instances, it is even directly redundant as written.
Ameren	Disagree	Change "BPS" to "BES" to be consistent with the rest of the document. The definition of Control Center has expanded significantly. We believe that the definition needs to focus more on the control aspects and not simply on the display of data. In the third bullet, the term "and asset management" needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. The Control Center should only include those facilities where NERC certified operators are required for its operation.
Black Hills	Agree	
TNMP	Agree	TNMP agrees with the proposed definition. The inclusion of multiple BES assets in the definition is important to help draw a distinction between Control Centers and substation HMIs.
NVEnergy	Agree	
MWDSC	Disagree	Alarm monitoring and processing, as well as coordination of restoration activities, is a real time function involving action by a Transmission or Generator Operator. Other entities may have redundant alarms at a facility, but will be contacted by the Transmission Operator as necessary to coordinate activities. Recommend adding a phrase to the definition such as ""A Control Center of a Transmission Operator or Generator Operator which is capable of performing ….."
Empire	Disagree	Optional definition: BES Control Center-A facility used to perform the function of an RC, BA, TOP, GOP or LSE in the real time operation of the BES.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	The problem again is what is the BES.
SCEG	Disagree	There is an opportunity for confusion between a "control room" at a power plant and a "control center", which only applies if two or more BES assets are being controlled. It would be better to use a more descriptive term such as "centralized control center" to more clearly indicate the distinction.
Exelon	Disagree	Exelon is concerned that the proposed definition may be interpreted by some to include dedicated generation plant control rooms (with more than one generator), as a result we recommend an exclusion statement be added to add clarification. We suggest the following be added: A control room shall not be categorized as a Control Center. A control room is typically located within the facility and operates control systems limited to controlling: A single generation plant with one or more generation units, A single transmission asset such as a transmission substation
BPA Trans	Disagree	This definition has the potential for making substation control houses or other facilities, where some type of control is exerted over more than one substation facility, be defined as a “control center.” Our definition for Control Center is: “The facility from which a power system is monitored and regulated. Dispatchers use computerized displays to match generation with load and to respond to faults in the system.” The NERC definition of Control Center should be consistent with what the Utility Industry normally uses to identify "Control Centers". We Suggest a more concise definition as follows: Control Center – “A Facility from which System Operators (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) monitor and control transmission or generation Facilities in real time.” The definitions of these terms from NERC Glossary of Terms Used in Reliability Standards, updated April 20, 2009 were considered and used to develop the recommended definition: System Operator Transmission Operator Transmission Generator Operator Telemetering

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		Facility Element
HQT	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
CCG	Disagree	The definition of Control Center as described is overly broad. Specifically, the second bullet unintentionally includes tagging systems or any display of generation management system data that does not have the ability to directly affect real-time operations. In addition, the words "asset management" should be removed from bullet three. Asset management is an overly broad term that could be unintentionally applied to generation management systems without the ability to directly affect real-time operations.
Allegheny Supply	Agree	
KCPL	Disagree	Disagree with the third bulleted item. Asset management has nothing to do with the maintaining the reliability of the BES. Recommend modifying the third bulleted item to, "System status monitoring and processing for reliability purposes".
Connectiv Energy	Disagree	This can be agreeable if the wording "multiple (i.e., two or more) BES assets) such as generating plants…" is not later interpreted to mean two or more BES Assets such as generating UNITS at a single plant.
MidAmerican	Disagree	This definition is not needed for two reasons. First, the existing non-CIP NERC standards have requirements for transmission control centers. Transmission control centers subject to those non-CIP NERC standards should be in scope. Second, if a generating unit is in CIP scope, then the Cyber Assets for the distributed control system for the generating unit should be evaluated to determine if they meet the criteria to be in CIP scope. Definition of a generation control center is not needed. The CIP standards must harmonize with and maintain the integrity of the other NERC standards. The proposed definition is problematic because it diverges from and possibly contradicts the other standards. If this definition were adopted in the Glossary, would the additional control centers it defines be subject to the other NERC standards for transmission control centers? If a definition is needed, it needs to be bright line, in contrast to the vague proposed definition. It must incorporate concepts of the other NERC standards for transmission control centers.
CPG	Disagree	The functions of a Control Center are too broad and will impact unintended operations centers, which do not have an effect on the BES.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
Santee Cooper	Disagree	Need some clarification concerning distribution control centers. SC does not want to classify it as a Control Center as it pertains to theses standards. It would cause unnecessary additional work and studies.
OGE	Disagree	OPTION: BES Control Center – a facility used to perform the function of an RC, BA, TOP, GOP or LSE in the real time operation of the BES.
Oncor	Disagree	Restated - A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES Facilities. Change BPS to BES in bullet 3
PPL Supply	Disagree	Comments: We mostly agree with EEI comments but would offer one additional clarification by adding the word "reliability" in EEI's proposed definition as per below: Parts of the definition are too broad. For example, a literal interpretation of: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations" Could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. We suggest: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time RELIABILITY operations"
St. George	Agree	
NGRID	Disagree	• Please explain BES Reliability Data • The whitepaper distinguished Control Rooms and Control Centers by number of geographic locations they control. • National Grid recommends changing the first bullet to "Supervisory control of geographically separated BES Subsystems" (see white paper) Also, change "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
MGE	Disagree	The qualifier of BES is in the definition of Control Center. But is missing in the forth bullet "Alarm monitoring and processing". Recommend that the forth bullet be completely removed, it allows for interpretation by regulators and does

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		not fit with the overall approach of the other BES level functions, it is a sub-set of SCADA.
FE	Disagree	1. The term "BES assets" is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: "A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations..." 2. For consistency, we recommend using BES, not BPS (see third bullet).
TECO	Disagree	We support EEI's Comments and wording changes. In addition we suggest: The term "BES Assets" in the definition of Control Center should be changed to "BES Subsystems."
CECD	Disagree	The references to generation plants and transmission substations should be replaced with the terms being defined, i.e. BES Generation Subsystem and BES Transmission Subsystem. The functions of a Control Center described are too broad and will unintentionally pull in operations centers that should be left out of the definition because they have little or no impact on the BES. This broad application goes against the purpose of the standard, which is to apply security controls commensurate with the potential impact to the reliability of the BES. One of the defining lines for determining if an entity is a BES user, owner or operator is whether the equipment is operated at 100 kV or above. A generation subsystem or transmission subsystem has a one line diagrams by which the connectivity can be evaluated. A control center is more appropriately considered a Cyber System to be evaluated in relation to BES Generation or BES Transmission Subsystems. CECD supports a definition of BES Subsystem that allow for flexibility by the registered entity to define their BES Subsystem, including the ability to exclude a control center as a BES Subsystem
MRO	Disagree	We feel the bullet "alarm monitoring and processing" should be removed, as this functionality should inherently be included as part of the other processes listed. In some instances, it is even directly redundant as written. We also feel the terms "generation plants" and "transmission substations" should be defined in the NERC Glossary of Terms, and "transmission facilities" should be replaced with "Transmission Facilities" to remove ambiguity.
GTC	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity. With respect to the first bullet of the definition, we suggest changing it to the following "Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control systems; or automatic load-shedding systems" We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		control center. The phrase "capable of" is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term "Situational awareness".
BGE	Disagree	Why is the term BPS used as opposed to BES? What is the definition of BPS as it is used here?
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	For the first bullet, consider striking reference to Automatic Generation Control (AGC) systems as this may cause confusion in ISO/RTOs where the scheduling agent may not be the operational organization responsible for the Generator Subsystem. Also, there are many cases where AGC controls only a small subset of the total MWs and may be used for sending market signals rather than for reliability. This definition as written would classify power marketers as Control Centers when they have no ability to access controls. Regarding the fifth bullet , consider striking entire line. Alarm monitoring and processing is not a control function. There may be operational groups within an organization that receive read-only alarms, but that may not have access to control system functions. Receiving an alarm or having the ability to monitor should not in and of itself make this a Control Center.
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	Parts of the definition are too broad. For example, a literal interpretation of: "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations" could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. An alternate definition suggestion is: "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time operations"
FMPA	Disagree	See FMPA's comments to 1.d. Use NERC Glossary defined terms: "BES assets" should probably become "Facilities"; "facilities" should become "Facilities" What does the "and system" refer to in the third bullet, "BES and system" since the BES is a system (Bulk Electric System)? Typo in this same third bullet, "BES" instead of "BPS"
Duke	Disagree	This definition should be revised to clarify that the definition of Control Center does not include the control room for a multiple unit site (which would be included as part of the Generation Subsystem). Need to delete the 4th and 5th bullets because "alarm monitoring and processing" and "coordination of BES restoration activities" are not associated with

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		functional control. Suggested wording: Control Center - A Facility for control of multiple (i.e. two or more) BES Subsystems. Functions that support real-time operations of a Control Center typically include one or more of the following: • Supervisory control of BES Subsystems, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems. • Acquisition, aggregation, processing, inter-utility exchange, or display of BES data required for BES reliability or operability. • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
NBSO	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing “A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations.” to “A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location.”
AESI	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity. With respect to the first bullet of the definition, we suggest changing it to the following ”Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control systems; or automatic load-shedding systems” We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a control center. The phrase “capable of” is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term “Situational awareness”.
IESO	Disagree	Third bullet should read "operability of the BES" not BPS. The fourth bullet regarding alarm monitoring should be more specific to the types of alarms monitoring and processing.
Manitoba 2	Disagree	This definition should refer to BES Subsystems, not BES assets, as currently written.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		Control Centres for small generation resources, below the NERC registration threshold (20 MVA), should be excluded from this definition, up to a defined total output aggregate. The Reliability Coordinator and Balancing Authority functions may need to be explicitly included in Attachment 2. Alarm monitoring and processing should be specific to operation and restoration functions of the Control Centre. The term “BPS” in the third bullet needs to be changed to “BES”. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	Alarm monitoring and data collection capabilities that do not and will not have remote supervisory control for BES assets should not be included in this definition. Many owners of facilities and BES assets monitor and collect information via SCADA; however, do not allow control of facilities and BES assets via SCADA. These owners should not be included in this Control Center definition. This separate line item should be removed from this definition.
ATC	Agree	
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table) **Security Function**

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.f. Comment (Response page 10)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>The definition of the Control Center should not be confused with identifying the tools used to perform critical functions. For example the mention of display of BES reliability or operation data does not make a control center as this data may be displayed as read only even in real time. In general the second bullet should be deleted from this definition.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA feels that the bullet “alarm monitoring and processing” should be removed. The term “processing” is ambiguous.
IMPA recommends the following changes to the definition:
Control Center - — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as Generation Subsystems or Transmission Subsystems. Functions that support real-time operations of a Control Center typically include one or more of the following:
• Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems</td></tr>
</table>

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		• Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS) • Coordination of BES restoration activities.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. Should further address the nuances regarding Control Centers that are not affiliated with specific generation plants or transmission substations. This would be appropriate for addressing the Control Center functioning as an RC, BA, or TOP. Midwest ISO Comments: The following changes need to be made to this definition: 1. The term "BES assets" is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: "A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…" 2. In the third bullet, the terms "and asset management" need to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term "BPS" should be replaced by "BES".
PacifiCorp	Disagree	This definition is not needed for two reasons. The term "control center," though not defined in the NERC Glossary of Terms, is already used in the context of other NERC reliability standards. For example, as defined in the NERC Glossary, a System Operator is an "an individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time. These control centers referenced in other NERC reliability standards should be the same as those defined by CIP standards. As currently drafted, the definition of Control Center will be different for CIP than for other NERC reliability standards. If it is needed, the current definition modified to remove the ambiguous language contained in the second bullet. Taken literally, this definition could include any BES reliability or operability display. PacifiCorp suggested modifying the definition to read: "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time operations."
PEPCO	Disagree	Parts of the Control Center definition are too broad. For example, a literal interpretation of - Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations - could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. Another example, a literal interpretation of - automatic load-shedding systems - could mean that a UFLS relay or a UVLS relay is a Control Center.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		We suggest the following: BES Control Center — A Control Center is capable of performing one or more of the functions listed below for two or more BES Generation Subsystems and/or BES Transmission Subsystem. Control Center functions that are used for real-time operations of the BES typically include one or more of the following: Bullet 1, Supervisory control of BES assets, including BES Generation Subsystems or BES Transmission Subsystem. Bullet 2, Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data used for real-time operations. Bullet 3, BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing BES information used by Responsible Entities to make operational decisions regarding reliability and operability of the BES). Bullet 4, Alarm monitoring and processing, should be changed to read BES alarm monitoring and processing.
NEI	Disagree	A) Clarify that the "Control Center" is not the control room of a multi-unit site (include in definition). It is expected that this "Control Center" is part of the transmission system. B) Delete the last two bullets. C) On third bullet, change BPS to BES. D) The open-ended nature and lack of clarity in this definition is concerning for the reasons described in the response to question 1a. This generally results from the approach of incorporating many technical functions into a single definition. As a result, there is a lack of clarity as to what is intended to be in scope and out of scope. For example, the descriptions could, perhaps unintentionally, even draw in plant control rooms or unit control rooms.

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures. or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures; or
- could hinder restoration to a normal condition.

Summary Consideration:

Organization	Yes or No	Question 1.g. Comment (Response page 11)
Progress Energy	Disagree	In 1st bullet, change to: "they could directly & immediately cause" For sub-bullets under 1st bullet add: “unacceptable risk to IROL” and remove or better define “BES separation; and/or a cascading sequence of failures.” Remove 2nd and 3rd bullets since the planning time frame and restoration doesn't impact real-time operational reliability. More generally, the scope of CIP standards should only address real-time cyber operations.
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		this definition should be eliminated in order to eliminate technical inconsistencies and confusion. Should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
GSOC/OPC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized? The use of the phrase “unacceptable risk” makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase “could … cause” is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase “could hinder” is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Hayden	Agree	
SDGE	Disagree	We propose changing the wording as follows for clarification: BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable: • they could directly cause, contribute to, or create – BES instability; and/or – BES separation; and/or – a cascading sequence of failures. If a “risk statement” is included in this definition, the ability to quantify the risk is required, e.g., significance of the risk and probability of the risk. Additionally, if a risk statement is made in the “High BES impact” case, then there should be a similar risk statement in the “Medium BES impact” case with objective criteria for establishing the difference between

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Medium and High. We propose deleting the second bullet item ("Planning time frame") in the definition, as it makes the analysis much more complicated without substantial BES Reliability benefit. Many entities lack the resources and tools to be able to incorporate power system planning studies into their NERC CIP work. If the "Planning time frame" bullet item is left intact as part of the definition, we would recommend that there be a stated single study timeframe and that studies be completed before a facility goes into service. This allows time to ensure equipment is in compliance. We also propose deleting the third bullet item in the definition ("could hinder restoration to a normal condition"), due to a lack of clarity. The definition of the phrase "normal condition" varies by entity and would bring about a lack of consistency with respect to this definition.
APPA	Disagree	APPA Task Force Comments: High Impact: The definitions of High, Medium and Low Impact must be based on how the industry plans and operates the Bulk Electric or Bulk Power System. Federal Power Act (FPA) Section 215(a)(4) defines "reliable operations" as: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." Bearing this definition in the EPAct in mind, the qualifier of "uncontrolled" should be added to "separation;" in other words, controlled or planned separation is not a High BES Impact. For all practical purposes, the definition of High BES Impact is embedded in the Criteria established in Attachment 1, so, the definition ought to include those criteria. In general, the criteria should be criteria correlated with a threat of an uncontrolled wide-area blackout such as the Northeast Blackouts of 1965 and 2003. The drafting team should consider adding this term along with Medium Impact and Low Impact to the NERC Glossary, since it could possibly be used for more than just this effort. Also, we recommend using the following term found in the NERC Glossary to describe what constitutes a High BES Impact event: "Adverse Reliability Impact" - The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. With regard to "restoration," we recommend that the SDT differentiate between conditions that "prevent" restoration versus merely "hinder" restoration. For a High BES Impact, we ought to be more concerned with "preventing" restoration than "hindering" restoration. The EPAct definition does not address restoration. Each blackstart unit and cranking path ought to be taken in context with the regional restoration plan. Most regional restoration plans have multiple black-start units and cranking paths. Unavailability of any single unit and cranking path is not a "High BES Impact," whereas loss of several resources may be categorized as "High." APPA Task Force Suggested Definition:

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		High BES Impact: BES Cyber Systems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable, has a high likelihood of resulting in an Adverse Reliability Impact to the BES.
Consumers	Disagree	We do not agree that there needs to be three different categories of impact. The concept of "Critical" or not, provided the "bright lines" that the SDT seemed to require. This three level approach, which is lacking a fourth, NO IMPACT, level, only seems to make the asset identification and categorization more complex and more subjective. In addition, the proposed changes seem to remove the ability to evaluate the impact the cyber system has on the BES. As proposed, the Cyber System inherits the same Impact Category as the BES Subsystem, so even minimal or no impact cyber systems/assets must be treated with the same requirements (CIP-003 >> CIP-009) as cyber systems that truly could have a substantial impact. This thereby dilutes the attention that should be paid to these critical systems and adds substantial time, effort and cost for compliance. The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Suggestion: Go back to the Critical Asset, Critical Cyber Asset process identified in the previous revisions
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be "merely guidelines" and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the "planning time frame" which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves. Finally, the word "hinder", which is ambiguous and subjective, should be changed to "prevent".
MPPA	Disagree	1. The term "unacceptable risk" is undefined, and leaves the definition open for interpretation. 2. This definition does not clearly quantify the difference between a High BES Impact system and a Medium BES Impact system in a manner consistent with Attachment 1. It is recommended that ", categorized in accordance with attachment 1," be inserted in the first line such that it reads as follows: "…BES Subsystems, categorized in accordance with attachment 1, have High BES Impact if …"
Central Lincoln	Disagree	The last bulleted item is not clear. Restoration from what condition? A small local outage? Central Lincoln agrees with the APPA Task Force comments on this definition, and suggest adding the word "uncontrolled" in front of "separation" so that controlled or planned separations are not included.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
NERC	Disagree	1. The phrase “unacceptable risk” is subjective, unauditable, and impractical to apply uniformly across entities. Further, it is contrary to the Commission’s directive in Order 706 paragraphs 139-156. 2. Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as “contribute to”, More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems.
Dominion	Disagree	It is difficult to accept new criteria without understanding the scope and impact of the proposed categories (high, medium and low) and without greater clarification of the details of the CIP-003 – CIP-009 revisions. If the intent of the high, medium and low categories is to establish VSLs and VRFs, such intent should be so stated by the SDT. Otherwise, Dominion suggests using two levels (high/low) as the use of three levels increases complexity without any added benefit. Dominion is also concerned about the use of the following subjective terms “unacceptable risk,” “hinder,” “could,” “would” and other similar terms. All of those terms should be clarified and implemented on an objective basis.
Encari	Disagree	“High BES Impact” is said to be any BES Subsystem that if destroyed, degraded or otherwise rendered unavailable would result in BES separation. The definition appears to include all BES Subsystems since any subsystem that is destroyed would necessarily be separated from the BES. We recommend that “further uncontrolled separation in the BES” replace the term “BES separation.”
US ACE – NW	Disagree	Define "hinder" in the statement "could hinder restoration to a normal condition." This is way too vague a statement and is essentially an unmeasurable item. Would a generator that was slow to start for blackstart assistance be fined for "hindering restoration" even though restoration was only slightly impacted? Need to have a definition that is measurable.
SCE	Disagree	SCE believes that the current definition for high impact BES systems does not bring sufficient clarity to the classification process and should be replaced by the criteria identified in Appendix 1 for making such determinations. SCE also requests clarification on certain ambiguous terms. For example, the term “hinder” is ambiguous and overly broad, as it is not defined by any reference to a duration or degree of impact. Similarly, the term “unacceptable risk” is ambiguous, as it is unclear which party’s assessment of risk will be respected. Finally, the duration of the “planning time frame” is unclear.
USBR	Disagree	It is not appropriate to classify an element as high in planning environment which is subject to numerous state condition assumptions. If the categorization is to be the result of a study, the sate conditions needs to be clearly defined. This term is not needed as High or Medium indicated an impact which would be sufficient to warrant analysis of associated cyber asset impacts. The term unacceptable risk should be eliminated as it is not defined in either how it is determined or the criteria of what would be considered unacceptable. The sentence addresses the potential without indicating a risk level.
Dyonyx	Disagree	It is recommended that the phrases “in a planning time frame” and “could hinder restoration” be specifically defined. These phrases add too much subjectivity to the definition without further detailed explanations.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Lastly, we believe the term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
Westar	Disagree	The phrase 'they could' in the first and second bullets is vague and leaves open room for interpretation. Suggest removing the phrase. 'could hinder restoration to a normal condition' - What is a normal condition? Need to clarify. Is it all lines, generators and load restored? Suggest either removing it or clarifying. Possibly tie to the 'cranking paths'.
Green Country	Disagree	A single event that will cause an Adverse Reliability Impact to the BES and cannot be stopped with an automatic protection system and/or manual operator intervention.
Oregon PUC		The terms “unacceptable risk of …” and “could hinder restoration” have too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
Manitoba 1	Agree	
Portland GE	Disagree	This definition is too broad and subjective terms such as “hinder” and “contribute” are not defined. In addition, the requirement does not contain a definition for “unacceptable risk,” which is subjective to each company – and to each auditor - therefore creating an inherent compliance risk. Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” This not only creates confusion, but may also then default everything into a “High” categorization, which would clearly contradict the intent behind the proposed risk framework. Clear, specific,

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		and technically defensible language is needed for this definition. From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required to be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is not an appropriate assumption. It is possible to have cyber systems which, if lost, degraded or compromised, will have no significant impact (or no impact at all, in some cases) in the function, operation or security of the BES subsystem that they support. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem.
PSEG		Comment #1: We do not agree with the use of the phrase “when destroyed, degraded”, because it does not align with the definition of BES Cyber System. BES Cyber System identifies a system compromised by an electronic means while “destroy” and “degraded” generally refer to a physical means of compromise (i.e. hammer, bomb or shotgun). Comment #2: We believe that more definition is needed for the term “planning time frame”. Is this intended to cover planned system outages, upgrades, additions and replacements? Comment #3: We believe that this reintroduces the concept of acceptable risk which was removed in CIP-002. Comment #4: We believe that more explanation of the term “cascading” is needed. Comment #5: We believe that any PM actions, projects, or system modifications could potentially hinder restoration to a normal condition. Comment #6: We believe that distinction should be made between “normal” condition and “operating” condition. Suggestion: “A Transmission or Generator Subsystem compromised through its BES Cyber System which could result in instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies). ” We do not believe that a planning time-frame is needed because the above definition would apply when performing engineering assessments in both the operational and planning time horizons. Restoration Issue: We also believe that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event. Restoration requirements should be consider separately in Attachment 1. We make this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis following a blackout event is completely different then analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s)

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments if the SDT disagrees with our suggestion: We are unclear as what the SDT means by the phrase “emergency, abnormal or restorative conditions, directly cause, contribute to, or create an unacceptable risk”. Although these individual terms may portray a sense of what the SDT is looking for they do not convey enough details for an entity to determine the performance level that needs to be prevented. - What criteria or threshold is applied to conclude “contribute to”? - What considerations should an entity use to identify “unacceptable” risk? - What is an “emergency” for the purpose of this standard? - Does “abnormal” mean any state other then all facilities in service? We believe that our suggested modifications provide a meaningful mechanism for entities, who wish to perform engineering analysis on those facilities listed in Attachment 1, to determine if a facility (Transmission Subsystem or Generation Subsystem) should remain in the identified category level (High or Medium) or be moved to a different category level (High, Medium or Low).
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. In addition, Wisconsin Electric Power Company feels the NERC glossary term Cascading should be used. Also, the term "planning time frame" is not clearly defined. Does this mean we have to make a new assessment for every unit outage and line outage? Wisconsin Electric Power Company recommends removing the language around the planning time frame.
Idaho Power	Disagree	“hinder restoration” is too vague. There are many things that can hinder but not prevent restoration that would not be considered high impact.
SOCO	Disagree	Is the first bullet point intended to refer to an Operational time frame (since the second refers to the Planning time frame)? If that’s the case, there will be times in light load periods, when multiple lines are out for maintenance, when the next outage could cause BES reliability concerns. This may not be the case for the exact same area of the system in the Planning time frame. Therefore, in the operations time frame, how would one identify and protect the specific subsystems when they might change on a daily basis? There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		and let those be the definitions and not have them up front at all. This is a standard whose sole purpose is to categorize cyber systems according to their impact on the BES so we can properly secure them. From V1 to now we've had to indirectly determine a cyber system's impact to the BES. We can't take into account any characteristics of the cyber system when we determine its BES impact. The standard requires that if a generation subsystem is high impact then all its associated cyber systems are high impact regardless of their actual impact to the generation subsystem. This will result in classifying most cyber systems higher than their actual impact. One suggestion is to determine the cyber system's impact directly against criteria similar Attachment 1. In essence ask "what is this cyber system's span of control?" and classify cyber systems based on how much of the BES they can control and adversely affect. A high impact cyber system can affect 10,000 MW's of generation or more than 50 transmission paths; etc. Under the definition for Medium BES Impact, we need to understand the difference between "directly cause" (shown in the High Impact) and "directly affect" (shown in the Medium Impact). If there is no difference, we suggest that the bullet points be introduced the same for both. Definition of High BES Impact – need a better understanding of what is meant by "could hinder restoration to a normal condition"; is the restoration to a normal condition directed toward a blackstart situation? Loss of a Transmission Subsystem could leave the power system in an abnormal state for an extended period of time (days/weeks) but does not mean that this situation is an unacceptable risk of instability, separation, or cascading failures. Loss of communication with a substation RTU (of a High BES Impact Transmission Subsystem) may hinder restoration to a normal condition should the need arise to control via the RTU while communication is down. We hope that this is not what was intended by the phrase "could hinder restoration to a normal condition". This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions.
DTE	Disagree	We are concerned that the term "unacceptable risk" is reintroducing the "acceptance of risk" concept that was removed from previous versions. The drafting team needs to define "planning time frame".
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current "one size fits all" approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	It is recommended that the phrases "in a planning time frame" and "could hinder restoration" be specifically defined. These phrases add too much subjectivity to the definition without further detailed explanations. Lastly, we believe the term "unacceptable risk" is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an "impact" analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		of the standard if the term “risk” is allowed to remain in the definition.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	N&ST is concerned that the phrase, "unacceptable risk" may be frequently subject to interpretation. In addition, what group or groups would make such a determination?
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	E ON U.S. recommends deleting the section: Any number of emergency or abnormal conditions, undefined as those situations are, could result in a situation in which nearly any BES subsystem could “contribute” to creating an unacceptable risk. The scenarios are only limited by one’s imagination. More objectivity is required in order to provide reasonable limits to the analyses.
Carthage	Agree	
WECC	Disagree	We feel this definition does a good job of defining situations that are a high impact to the BES, however, it continues to provide open ended language such as “could directly” that does not provide adequate clarity on if something should be considered an impact or not. What does contribute to or cause unacceptable risk mean? How is unacceptable judged? What was the intent of the term “planning time frame”?
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a. CenterPoint Energy believes the “Critical Asset” definition in the current version of CIP-002 should be retained. However, CenterPoint Energy would support the SDT incorporating the proposed characteristics of “High BES Impact” into the requirements or definition of “Critical Assets” in version 4. Likewise, some of the concepts found in Attachment 1 could be useful for putting some more specificity into the risk based assessment methodology for determining Critical Assets. However, Attachment 1 would need some refinement. Please refer to

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		CenterPoint Energy's comments to question 8.
LCRA	Disagree	The "planning time frame" needs to be defined.
FRCC	Disagree	This also uses the term "degraded" which is ambiguous. See previous comment. In addition, the first bullet uses the terms "unacceptable risk". Who determines what is unacceptable? This is not easily monitored by compliance enforcement authorities and would likely lead to interpretation requests. If the drafting team has knowledge of what they consider to be unacceptable, they should clearly state it. The first bullet has includes "BES" instability, and "BES" separation, why do the sub-bullets in the planning time frame not refer to "BES" ?
NIPSCO	Disagree	We believe that more clarity is needed for the term "planning time frame". Is this intended to cover planned system outages, upgrades, additions and replacements? An entity could interpret any maintenance actions, projects, or system modifications could potentially hinder restoration to a normal condition. Additionally, we believe that this reintroduces the concept of acceptable risk which was removed under FERC order 706. Suggestion: Clarify the intent of the term planning time frame and remove references to unacceptable risk.
ConEd	Disagree	There should be a 'High BES Impact' category that deals with Control Center-type systems and then a lower level that deals with Transmission Substations. To place a control center and a substation in the same category level is not in the direction we should be heading. Individual Transmission Substations simply are not as important as area Control Centers.
EEI	Disagree	EEI believes that the current written definition for high, impact BES systems does not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in an (amended) Appendix 1 to make such determinations. Restoration Issue: EEI also believes that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event. Restoration requirements should be considered separately in Attachment 1. We make this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis following a blackout event is completely different then analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Alternative strategies will need to be identified for entities with flexible blackstart plans, e.g. multiple Blackstart units

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		with multiple cranking paths. Reliability of the BES is not advanced by creating significant compliance liability for those organizations that have already invested in developing a flexible and resilient blackstart strategy. The “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats.
O&R	Disagree	There should be a ‘High BES Impact’ category that deals with Control Center-type systems and then a lower level that deals with Transmission Substations. To place a control center and a substation in the same category level is not in the direction we should be heading. Individual Transmission Substations are not as important as area Control Centers.
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "High BES Impact". The words "contribute to" need to be removed. What is meant by "a cascading sequence of failures"? We suggest that this term should be replaced with "widespread outages". We doubt that SERC, NERC, and FERC would agree on what an acceptable or unacceptable risk would be after an event would have occurred. We believe a MW threshold for load lost should be established that would define a High BES Impact, such as 300 MW other than consequential load, consistent with the threshold for a NERC reportable event under NERC EOP-004 and also the threshold for the DOE Energy Emergency Incident and Disturbance Reporting Requirement per Form EIA-417. Alternatively it would suffice to identify IROL as High BES impact. The last statement in the definition "could hinder restoration to a normal condition" is too broad of a statement for a definition; it needs to be classified as Low or Medium BES Impact. From the perspective of a system restoration from a full blackout condition, the loss of any asset could "hinder" the restoration to a normal condition.
Black Hills	Disagree	Need definition of "could", "Contribute to", and "unacceptable risk". Current CIP-002-1 guidance is that the probability = 1, therefore "could" will always happen. "planning time frame" needs to be defined. A lot can happen in ten years - which is one of our planning time frames. Is "abnormal" limited to N-3? Need to define "hinder" - how much is of significance?
TNMP	Disagree	TNMP has a concern regarding the current definition. High BES Impact would be defined in the official NERC glossary, and categorized by the criteria in CIP-002 Attachment 1. The definition needs an additional “AND”, not “OR”, bullet statement of “further constrained by the criteria in CIP-002 Attachment 1.” By having a definition and a criteria it gives auditors two places to look to determine impact of a BES Subsystem. Currently, the criteria fail to properly address facilities with joint ownership. Could an auditor use the current definition to help clarify where the criteria is lacking in real world applications? TNMP believes this concern needs to be addressed by the drafting team with certainty. TNMP has experienced auditors and attorneys utilizing strict application of actual

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		standard text, rather than referencing discussions and guidance surrounding development of the standards.
NVEnergy	Disagree	While we appreciate the efforts of the Drafting Team to characterize the qualities of a High Impact Subsystem, as written, these qualities are still excessively vague. For instance, one could easily conclude that any unavailable BES subsystem "could hinder restoration to a normal condition". What degree of hindrance is specified here? Technically, any abnormal condition represents some hindrance to the restoration of a system to normal condition. As with the existing paradigm of the present CIP RBAM practice, there continues to be a lack of needed specificity in classification of assets/subsystems. The concepts described in this proposed definition appear to have some merit, but the difficulty comes about when the entity goes to make a determination.
MWDSC	Disagree	Unclear who determines what "unacceptable risk" is? Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding the adjective "interconnected" before the term BES under each bullet. For example, "risk of interconnected BES instability" Also, need more specific criteria such as in Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Disagree	Optional definition: A single event that will cause and Adverse Reliability Impact to the BES and cannot be corrected with an automatic protection system and/or manual operator intervention.
NCEMCS	Disagree	"could hinder restoration to a normal condition" - This is an open ended statement and needs a better clarification of the actual conditions. For example, if some condition destroyed all communications at a BES facility but it was possible to restore service manually, this definition could hinder restoration.
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Agree	
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for "BES Impact" such as "BES subsystems that if destroyed, degraded, or otherwise rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines provided in Attachment 1 of this Standard." Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.
BPA Trans	Disagree	1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		makes sense, but: "BES Cyber Systems need to be “secure” not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", "unacceptable risk," or “hinder restoration.” In particular, what is, and how long is a "planning time frame"? 3. It is unclear why the second and third conditions (bullets) removes the reference to the BES. Is this referring to the BES, a single BES subsystem? There is no way of knowing what the intended referent is. 4. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is “destroyed, degraded or otherwise rendered unavailable.” But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of “Subsystems whose destruction, degradation, or lack of availability could lead to …” The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
Allegheny Supply	Disagree	
KCPL	Disagree	This is too broad with regard to “BES Subsystems”. There will always be a “tipping” point of generation and transmission outages, that, when crossed, yields an unreliable and undesirable operating condition. As an example, any combination of generating facilities within the Eastern interconnect that totals half of the generation meeting load demand, if removed from service, would be devastating to the operation of the BES. The way this is written, all generating facilities would have to be included as a HIGH. The same illustration could be used for transmission facilities. In addition, placing the burden of establishing the loss of a facility or group of facilities on the Reliability Coordinators and the reliability impact is a concern as they do not have the resources to manage the likely flood of requests and endless operating configurations that would result from Registered Entities seeking relief from this CIP Standard.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	The definition, as stated here and without the specific guidance provide in the Standard, provides criteria that most Generation Owners can not determine – but that most Transmission Operators can determine. This exacerbates the issue exiting with the current version of the standards. This noted, the criteria included in the Standard provide a clear set of lines for making the classification. As such, this is acceptable if the definition includes the reference to the criteria as the means to make the determination. What will be the definition of unacceptable risk? What is the reason for further breaking down the BES into these categories (high, medium, low)? Is this to better categorize Critical Assets? More categories do not necessarily benefit Critical Asset determination. Coordination between the GO/GOP and the TOP is currently the main driver for Critical Asset determination. Establishing more categories will likely add another unnecessary level of complexity.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If a new definition is created, the scope should be limited to “direct” causes and exclude “in the planning time frame.” Planning timeframe is vague and varies. As proposed, it cannot be consistently implemented or fairly audited. The standard should address the current rating and impact, not a potential future impact.
CPG	Disagree	This definition takes into account BES Subsystems if, when destroyed, degraded or otherwise rendered unavailable could hinder restoration to a normal condition. If this term is used solely with Critical Infrastructure Protection, then why would cyber assets be included in restoration, given that they will most likely not be functioning during a blackout? Furthermore, the term “unacceptable risk” is not well defined. It is vague and needs further defining.
Santee Cooper	Disagree	High impact should be left to be concerned with actual threats of uncontrolled wide area blackouts. This is the most important Impact and it should always be treated as such, and should not have problematic items such as “hindering” or short term risks…When there are viable alternatives to BES problems, such as Blackstart Unit alternate cranking paths, we should not Carte Blanche all Blackstart Units into the High Impact arena. Attachment 1 definitively needs further work. You don’t want to trivialize the High Impact, so only those items that have an absolute impact should be on the high impact listings.
OGE	Disagree	• Provide the exact duration of a “planning time frame”. • The term “contribute to” is too discretionary. • A metric is needed to know what "unacceptable" or "hinder" means. • Why is the term “BES” excluded in the second bullet above? (BES instability). What is the difference between “BES instability” and “instability”? What is the difference between “BES separation” and “separation”? What is the definition of “instability”?

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		• "Normal condition" needs to be defined in this context. • OPTION: A single event that will cause an Adverse Reliability Impact to the BES and cannot be stopped with an automatic protection system and/or manual operator intervention.
Oncor	Disagree	The enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1. Remove from Definition of Terms section.
PPL Supply	Disagree	Comments: A more precise definition of Black Start generating units is needed that in the proposed Rev. 4. To say that "Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem." is inadequate to identify only those generating units that are used for initial restoration of the BES. System restoration plans normally identify all units from the blackstart initiating through the thermal generation at the end of the cranking path, including any intermediary units, so clarification is needed to avoid misinterpretation.
St. George	Agree	
NGRID	Disagree	Reference to BES Cyber system should be made since the Transmission/Generation subsystems will be degraded or destroyed through BES Cyber System (intent of the standard). Also, it is recommended to consider an alternate phrase/word to "destroyed/degraded" as they are generally referred to a physical means of compromise. "BES Subsystems have High BES Impact if, when "compromised" through its BES Cyber Systems, they could:…" If the SDT decides to keep the current definition, then answers to following questions are required - What criteria or threshold is applied to conclude "contribute to"? - What considerations should an entity use to identify "unacceptable" risk? - What is an "emergency" for the purpose of this standard? - Does "abnormal" mean any state other then all facilities in service?
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1.
FE	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three BES Impact buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. This High BES Impact definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. For example, it is subjective as to why only a 2000MW and above generation Subsystem threshold would be screened for High BES Impacts. The focus should be evaluating generation Subsystems, regardless of the MW value tripped, that

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		could lead to a High BES Impact result. FE suggests an approach that creates greater clarity and a "bright line" as to what is deemed to be a High BES Impact; meaning that the standard focus only on those threats that could lead to a High BES Impact (cascade, system separation, instability, restoration concerns) and drive greater uniformity in the industry on how we land there. To move beyond that into classifying a Medium BES Impacts and certainly Low BES Impacts is not needed. We also offer a specific edit to the High BES Impact definition. The second bullet is largely redundant to the first bullet, causes confusion and not needed. FE suggests that the second bullet be removed.
TECO	Disagree	The amended Attachment 1 categorization definition (see EEI comments) should be used in place of this, as it is more clearly defined. If that cannot be accomplished, references to the “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a reliable cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. The terms “unacceptable risk”, “abnormal” and “hinder” need to be more clearly defined, to avoid confusion and misinterpretation. Additionally, we support EEI’s comments on restoration issues.
CECD	Agree	Agreement with the definition is based on the registered entity having the independence to define its BES subsystems.
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.
GTC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized? The use of the phrase “unacceptable risk” makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase “could … cause” is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase “could hinder” is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		"commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose. With respect to the second bullet, it is unclear what is meant and it needs to be clarified.
Xcel	Disagree	The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion. The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1. There is a need to have a definition of “unacceptable”. What criteria do you use to determine if a risk is unacceptable?
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 h, 1i should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. “Cascading Sequence of failures” is not clearly defined In the phrase, “Or could hinder restoration to normal condition”, normal condition is not clearly defined. Please clarify what is meant by planning time frame. “Unacceptable risk” not well defined. It is vague and should be linked to NERC transmission planning standards. Also, please note response to Q3.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Regarding “High BES Impact” and “Medium BES Impact” references to the “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. Consider striking references to “planning time frame” and replace with “based on analysis of real-time operating conditions.”

Organization	Yes or No	Question 1.g. Comment (Response page 11)
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	AP believes that the current written definition for high impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations. AP also believes that this reintroduces the concept of acceptable risk which was removed in CIP-002.
FMPA	Disagree	We applaud the SDT in nearly correctly identifying the criteria for which High BES Impact should be determined in alignment with the definition of Reliability in the Energy Policy Act of 2005. The FPA Section 215(a)(4) defines “reliable operations” as: “operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” This FPA definition is almost synonymous with the definition of Adverse Reliability Impact in the NERC Glossary of terms: “(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection”. FMPA recommends using the NERC Glossary to simplify the definition. Bearing this definition in the FPA and Glossary in mind, the qualifier of “uncontrolled” should be added to “separation”; in other words, controlled or planned separation is not a High BES Impact. FMPA recognizes that Adverse Reliability Impact does not address restoration whereas High Impact ought to. However, there is a difference between “hindering” and “preventing” restoration. For a High BES Impact, we ought to be more concerned with “preventing” restoration than “hindering” restoration. Each blackstart unit and cranking path ought to be taken in context with the regional restoration plan. Most regional restoration plans have multiple black-start units and cranking paths. Unavailability of any one is not a “High BES Impact,” whereas loss of several may be. For all practical purposes, the true definition of High BES Impact is embedded in the Criteria of Attachment 1, so, the definition ought to include those criteria. In general, the criteria should be criteria correlated with a threat of an uncontrolled wide-area blackout such as the Great Northeast Blackouts of 1965 and 2003. Therefore, the definition of “High Impact” would have more clarity by saying: “BES Cyber Systems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable, has a high likelihood of resulting in an Adverse Reliability Impact to the BES, or could prevent restoration efforts.”
Duke	Disagree	This definition is not needed because Attachment 1 of the standard describes High BES Impact in great detail.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized?

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		The use of the phrase “unacceptable risk” makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase “could … cause” is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase “could hinder” is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
IESO	Disagree	The term "risk" is misused in the phrase "unacceptable risk of". the term should refer to the "unacceptable likelihood of"
Manitoba 2	Disagree	This definition very closely resembles the Risk Factors defined in the NERC Reliability Standards Development Procedure, which are used to develop Violation Risk Factors (VRFs), which is redundant, and is not consistent with the impact criteria described in Attachment 1. The definition “High BES Impact” should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. It is unclear what is meant by “in a planning time frame” and this point should be removed. The standard is limited to systems that are already in-service. Please define emergency, abnormal, or restorative conditions. Restoration should be categorized as “Medium BES Impact”. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	ATC does not agree with the use of the phrase “when destroyed, degraded”, because it does not align with the definition of BES Cyber System (Either ATC or the SDT definitions). BES Cyber System identifies a system compromised by an electronic means while “destroy” and “degraded” generally refer to a physical means of compromise (i.e. hammer, bomb or shotgun). Suggestion: “A Transmission or Generator Subsystem compromised through its BES Cyber System which could result in instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies). ” ATC does not believe that a planning time-frame is needed because the above definition would apply when performing

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		engineering assessments in both the operational and planning time horizons. An alternative suggestion would be for the SDT to use the existing NERC Event category. Category 5 event is High Category 5 An event resulting in one or more of the following: a. The loss of load of 10,000 MW or more. b. The loss of generation of 10,000 MW or more. Category 4 event is Medium Category 4 An event resulting in one or more of the following: a. The loss of load from 1,000 MW to 9,999 MW (excluding SPS/RAS as noted in Category 2, UFLS, or UVLS actuation). b. Unintended system separation resulting in an island of a combination of load and generation of more than 10,000 MW. Category 3 event is Low Category 3 An event resulting in one or more of the following: a. The loss of load from 500 MW to 1,000 MW (excluding SPS/RAS, UFLS, or UVLS actuation). b. The unplanned loss of generation (excluding automatic rejection of generation through SPS/RAS as noted in Category 2) of 2,000 MW or more in the Eastern Interconnection or Western Interconnection, and 1,000 MW or more in the Texas or Québec Interconnections. c. Unintended system separation resulting in an island of a combination of load and generation of 5,001 MW to 10,000 MW. Category 1 or 2 is excluded from CIP-003 - 009. Restoration Issue: ATC also believes that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event. Restoration requirements should be considered separately in Attachment 1. ATC makes this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		following a blackout event is completely different than analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit as high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments if the SDT disagrees with our suggestion: ATC was unclear as what the SDT means by the phrase “emergency, abnormal or restorative conditions, directly cause, contribute to, or create an unacceptable risk”. Although these individual terms may portray a sense of what the SDT is looking for they do not convey enough details for an entity to determine the performance level that needs to be prevented. - What criteria or threshold is applied to conclude “contribute to”? - What considerations/criteria should an entity use to identify “unacceptable” risk? - What is an “emergency” for the purpose of this standard? - Does “abnormal” mean any state other than all facilities in service? ATC believes that our suggested modifications provide a meaningful mechanism for entities, who wish to perform engineering analysis on those facilities listed in Attachment 1, to determine if a facility (Transmission Subsystem or Generation Subsystem) should remain in the identified category level (High or Medium) or be moved to a different category level (High, Medium or Low).
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems

Organization	Yes or No	Question 1.g. Comment (Response page 11)

for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)

Organization	Yes or No	Question 1.g. Comment (Response page 11)
PSE	Disagree	The definition should focus on the level of disturbance the BES Subsystem could cause if destroyed or degraded. It is unclear what "in a planning time frame" is intended to mean. Further Puget Sound Energy supports EEI's comments relative to exclusion of restoration activities included black start generation and cranking paths for reasons 1) not all entities need or have blackstart units, 2) they could be identified for local customer support versus interconnection support and 3) the complexity associated with the flexibility in cranking that a restoration plan must address due to the varying scenarios that could occur which makes it difficult to determine one or two critical paths.
IMPA	Disagree	The Standard and Attachment 1 both define what constitutes a High BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a High BES Impact. In addition, the definition needs to be removed because it uses the term “unacceptable risk” which could have various meanings depending on an individual’s judgment.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. In the 1st bullet, ERCOT ISO requests clarification of “unacceptable risk”. This is a very ambiguous requirement and lends itself to subjective interpretation by the Responsible Entity and an audit body. Recommend that the drafting team consider returning to the use of the definition of Adequate Level of Reliability in determining risk tolerance. ERCOT ISO recommends removing the 2nd bullet or at least differentiating between operating and system planning time horizons. Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
PacifiCorp	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Subsystems that may have a high impact in the planning time frame. The standard should address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The High BES Impact definition appears to mimic the definition of a High Violation Risk Factor. We question why there is a need to consider "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation.
PEPCO	Disagree	The current definition for High BES Impact does not bring sufficient clarity for determining the appropriate category. There needs to be a bright-line between High BES Impact, Medium BES Impact, and Low Impact. For High Impact, it appears to be risk based. How are BES instability, BES separation, and a cascading sequence of failures pre-determined or defined? Could all BES systems hinder restoration to a normal condition? What is meant by hinder or normal condition? More clarity is need for the term "planning time". Differentiating between High, Medium and Low BES Subsystems may have little value or credibility for associated cyber security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. We suggest the following: Do not use High, Medium, or Low. If cyber control system first approach is use, we would offer that the high, medium, or low would not be needed. Appropriate security measures/requirements would be based on platform of in-scope BES cyber control systems, the connectivity of the asset (TCP/IP vs. dial-up vs. not connected), and/or the span of control of the cyber asset's impact. If the SDT feels that this term is still required, suggest the you use only the criteria identified in an (amended) Appendix 1 for the definition.
NEI	Disagree	A) In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three BES Impact buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. This High BES Impact definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		may not result in the system impacts included in this definition. For example, it is subjective as to why only a 2000MW and above generation Subsystem threshold would be screened for High BES Impacts. The focus should be evaluating generation Subsystems, regardless of the MW value tripped, that could lead to a High BES Impact result. NEI suggests an approach that creates greater clarity and a "bright line" as to what is deemed to be a High BES Impact; meaning that the standard focus only on those threats that could lead to a High BES Impact (cascade, system separation, instability, restoration concerns) and drive greater uniformity in the industry on how we land there. To move beyond that into classifying a Medium BES Impacts and certainly Low BES Impacts is not needed. B) We also offer a specific edit to the High BES Impact definition. The second bullet is largely redundant to the first bullet, causes confusion and not needed. NEI suggests that the second bullet be removed. C) Since cyber security is not the focus here, this has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security. D) It is recommended that Attachment 1 (as modified by comment A)) be used to provide an adequate definition, and that the Glossary be point to the Attachment. E) If the definition is to be kept, provide clarification for the terms "unacceptable risk" and ""could hinder". F) Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the Appendix). While the current "one size fits all" approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

Summary Consideration:

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Progress Energy	Disagree	Keep only the 2nd bullet as-is. Remove 1st bullet "directly affect the electrical state or the capability of the BES;" – it is too vague and would cause varying interpretations. Remove 3rd bullet "in a planning time frame, under emergency, abnormal, or restorative conditions, – directly affect the electrical state or the capability of the BES; or – directly affect the ability to effectively monitor and control the BES." – Scope of CIP standards should only address real-time cyber operations.
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The third bullet of the definition is largely redundant to the first two bullets and improperly references "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". This is not reasonable and this definition needs to be revised significantly. Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
GSOC/OPC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Hayden	Disagree	This is a confusing definition. The term "...directly affect..." can also be applied to the definition of "HIGH BES Impact." As such, I wonder if this can be rewritten to help place the impact on the right layer of the impact continuum. Can it be more specifically related to the BES Adequate Level of Reliability (ALR) requirements? This definition would be very difficult to enforce with the current level of criteria.
SDGE	Disagree	In addition to the lack of a “risk statement” in this “Medium BES impact” definition, what is the difference between, “causing, contributing to, or creating, unacceptable risk to the BES” (in “High impact”) and “directly affecting the electrical state or capability of the BES” (in “Medium impact”)? Why is the risk of something happening to the BES deemed a higher impact than “directly affecting” the BES? This definition for “Medium” doesn’t provide much granularity or difference between that of “High BES impact”. We propose a more binary approach with respect to BES impact, namely having “BES impact” and “no BES impact” choices (re-working the “high impact” and “low impact” definitions). Currently, the way the three different impact choices are defined (H, M, L), will unnecessarily complicate drafting and implementing the CIP-003 through CIP-009 Standards. For example, would requirements for access to “High BES impact” assets be different than the requirements for access to “Medium BES impact” assets? Would information associated with high impact BES Subsystems have different requirements than information associated with medium impact BES Subsystems? Would training requirements be different for the aforementioned BES classifications? Would vulnerability assessments be lesser in scope or less frequent in occurrence for medium impact BES classifications versus that of high impact BES classifications. This imprecision would confuse implementation and increase the administrative cost of compliance without increasing BES security. We are proposing having just two choices for BES Impact (BES Impact, and no BES Impact).
APPA	Disagree	APPA Task Force Suggested Definition: Medium BES Impact: BES Cyber Systems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could cause a post-contingency system state in which an additional single contingency is likely to result in an Adverse

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Reliability Impact to the BES.
Consumers	Disagree	If the SDT is unwilling to return to the Critical Asset, Critical Cyber Asset process identified in the previous revisions, then this category should be renamed "Low" impact, and the currently proposed low impact should be re-identified as "No Impact". This would allow the SDT and REs to focus on assets and cyber systems that truly have an impact and dismiss those that do not.
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be "merely guidelines" and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the "planning time frame" which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves.
MPPA	Disagree	1. This definition could be equally applied to High BES Impact. A system that can affect the electrical state of capability of the BES, could impact the stability of the BES, there by falling under the definition of a High BES Impact. 2. This definition does not clearly quantify the difference between a High BES Impact system and a Medium BES Impact system in a manner consistent with Attachment 1. It is recommended that ", categorized in accordance with attachment 1," be inserted in the first line such that it reads as follows: "…BES Subsystems, categorized in accordance with attachment 1, have Medium BES Impact if …"
Central Lincoln	Agree	
NERC	Disagree	Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as "contribute to", and "create an unacceptable risk". More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems.
Dominion	Disagree	Dominion does not agree with including the statements "directly affect the electrical state or the capability of the BES" and "directly affect the ability to effectively monitor and control the BES" in the definitions of "Medium BES Impact" and "Low BES Impact." Every physical generation or transmission asset has the ability to directly affect the electrical state or the capability of the BES. Therefore, by default, all such assets would all be classified as Medium BES Impact. To the extent these devices are monitored, each directly affects the ability to effectively monitor the BES. The term "electrical state" should be clarified.
Encari	Disagree	"Medium BES Impact" is said to be any BES Subsystem that if destroyed, degraded or otherwise rendered unavailable could directly affect the electrical state or the capability of the BES. The definition appears to include all BES Subsystems

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		since any subsystem that is destroyed would necessarily affect the capability of the BES. We recommend that "adequate level of reliability" replace the term "capability." "Adequate level of reliability" of the BES is a term with an established meaning. NERC defined the term "Adequate level of reliability" on May 5, 2008 in a filing with FERC.
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the current definition for medium impact BES systems does not bring sufficient clarity to the classification process and should be replaced by the criteria identified in Appendix 1 for making such determinations. SCE also requests clarification on certain ambiguous terms. For example, it is unclear to SCE what the meaning of "electrical state" is, as that term is not defined in the NERC Glossary of terms. The duration of the "planning time frame" is also unclear.
USBR	Disagree	The term "electrical state or capability" it too vague to help determine what is a medium impact. It would be better relate the medium state to the terms used in high with a degree of separation. This term could imply that any change in the BES irrespective of the durability of the BES under those conditions would be a medium impact. This would mean that any event would be considered a medium impact irrespective of the true reliability of the BES immediately following the event.
Dyonyx	Disagree	The proposed definition uses undefined terms ("electrical state", "planning time frame") and is too subjective. In addition, we do not believe the term "capability" is appropriate. The loss of even 10 MW will impact the total "Capability" of the regional system, but this is not the intent of the standard.
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The third bullet of the definition is largely redundant to the first two bullets and improperly references "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". This is not reasonable and this definition needs to be revised significantly. Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Westar	Disagree	Again the phrase 'they could' is vague. Suggest removing. The first bullet is very vague. What is meant by 'directly affect the capability of the BES'. We need this more clearly defined.
Green Country	Disagree	A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES.
Oregon PUC	Disagree	The language “could directly affect …” seems overly broad. Clear, specific and technically defensible language is needed for this definition.
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree with this definition, and incorporates by reference the same comments as for the High BES Subsystem definition. This definition is too broad and subjective terms such as “hinder” and “contribute” are not defined. In addition, the requirement does not contain a definition for “unacceptable risk,” which is subjective to each company – and to each auditor - therefore creating an inherent compliance risk. Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” This not only creates confusion, but also may then default everything into a “High” categorization, which would clearly contradict the intent behind the proposed risk framework. Clear, specific, and technically defensible language is needed for this definition. From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is not an appropriate assumption. It is possible to have cyber systems which, if lost, degraded or compromised, will have no significant impact (or no impact at all, in some cases) in the function, operation or security of the BES subsystem that they support. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem.
PSEG	Disagree	Comment #1: The phrases “directly affect”, “electrical state” and “effectively monitor” does not convey sufficient clarity for entities to properly identify BES Subsystem which should fall into this category. We offer the following three options for the SDT to consider: b) Delete this classification and keep only the “High” and “Low” classifications. c) Provide more specificity to the term in order for entities to understand what is the potential impact of facilities classified as “Medium”. d) Do not define the term Medium BES Impact but identify those facilities that fall under this classification level. (Allow

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		entities to use the same engineering assessment identified for "High BES Impact" to determine if the facilities should be moved to either "high" or "Low". Option 1: This option allows the team to focus on those BES Cyber Systems that truly have a high impact on the BES. Option 2: If the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could directly affect the electrical state or capability of the BES? - Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?) - See our comments under High BES Impact for the phrase "under emergency, abnormal, or restorative conditions". Option 3: This would eliminate the need for the SDT to define Medium BES Impact and allow entities the options to use an engineering assessment to either raise or lower those BES Cyber Systems that have been identified in Attachment 1. Example: If an entity could demonstrate through an engineering assessment that a facility identified as Medium BES Impact would not cause instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies) then that facility could be identified as "Low". Comment #2: We fail to see the difference between "directly affect the electrical state or the capability of the BES" in Medium BES Impact and the first bullet in High BES Impact.
WE-Energies	Disagree	Wisconsin Electric Power Company feels there should be additional information provided as to what "electrical state or capability" means. This should include how this risk level would actually impact the BES. In addition, Wisconsin Electric Power Company agrees with EEI's comments regarding this definition.
Idaho Power	Disagree	Too vague. Every BES Subsystem has some affect on the electrical state of the BES. Too much room for subjectivity on what directly or indirectly affects the BES.
SOCO	Disagree	There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each and let those be the definitions and not have them up front at all. Under the definition for Medium BES Impact, we need to understand the difference between "directly cause" (shown in the High Impact) and "directly affect" (shown in the Medium Impact). If there is no difference, we suggest that the bullet points be introduced the same for both. Definition of Medium BES Impact – need a better understanding of what is meant by "directly affect the electrical state or capability of the BES" and "directly affect the ability to effectively monitor and control the BES". The phrase "directly affect the ability to effectively monitor and control the BES" seems to apply more to a Cyber System rather than a BES Subsystem. It is the Cyber Systems that allow the ability to monitor and control the BES not the BES Subsystems

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		themselves. This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions.
DTE	Disagree	The drafting team needs to define “planning time frame”.
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a “No BES Impact” should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	The proposed definition uses undefined terms (“electrical state”, “planning time frame”) and is too subjective. In addition, we do not believe the term “capability” is appropriate. The loss of even 10 MW will impact the total “Capability” of the regional system, but this is not the intent of the standard.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	It is not clear to us what distinguishes "directly affect the electrical state or capability of the BES" from the previous (High) impact definition.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	Under emergency or abnormal conditions, undefined as those situations are, nearly any BES subsystem could “contribute” to creating an unacceptable risk. The scenarios are only limited by one’s imagination. More objectivity is

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		required. E ON U.S. again recommends deleting the planning time frame bullet and sub-bullets.
Carthage	Agree	
WECC	Disagree	This does not provide additional clarity. See previous comment (1.g).
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a. It is particularly hard to imagine what rationale there would be for attempting to distinguish medium and low impact facilities (setting aside the "subsystem" quagmire). Virtually any non-radial asset, if damaged, would affect the "electrical state" of the BES by, if nothing else, removing one or more network elements. Likewise, one could argue that loss of a single telemeter, let alone an entire unit at one substation, directly affects the ability to monitor and control the BES, although one could argue about the meaning of "effective" monitoring and control. If the basic intent of the SDT is to apply some set of requirements for every cyber asset, regardless of criticality, the SDT should simply propose such a set of requirements rather than introducing this proposed paradigm.
LCRA	Disagree	1. The "planning time frame" needs to be defined. 2. The phrase "directly affect" should be changed to "directly and adversely affect". The original phrase is too broad.
FRCC	Disagree	See previous comments on use of the term "degraded". In addition, the first bullet uses the terms "electrical state" or "capability" of the BES . These terms are very broad and can mean a number of different things to different people. It should be clear what is expected here.
NIPSCO	Disagree	We believe there is not enough distinction between High and Medium BES impact. There appears to be overlap within the definitions and this overlap will create confusion and a variety of interpretation issues. Suggestion: Review the definitions of High and Medium and provide an increased distinction between the two criteria.
ConEd	Agree	
EEI	Disagree	EEI believes that the current written definition for medium impact BES systems does not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in an (amended) Appendix 1 to make such determinations.
O&R	Agree	
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of Medium BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "Medium BES Impact". This definition is again too broad, to what order of

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		magnitude to "directly affect the ability/electrical state" refer. The loss of any asset or subsystem would affect the BES but to varying magnitudes. An explanatory statement should be added such as "directly affect the electrical state or capability of the BES to maintain established voltage conditions within 3% of normal system conditions." We believe that we need a MW threshold for load lost that would qualify for Medium BES Impact, such as more than 100 MW but less than 300 MW other than consequential load.
Black Hills	Disagree	Need definition of "could". Current CIP-002-1 guidance is that the probability = 1, therefore "could" will always be a possibility. "planning time frame" needs to be defined. A lot can happen in ten years - which is one of our planning time frames. Concern about meaning of "directly" as compared to "indirectly" - what is the significance? Definition of "capability of the BES"?
TNMP	Disagree	Comments on High BES Impact are equally applicable to this definition.
NVEnergy	Disagree	As with the above “High Impact” comments, the same applies here as well. Beyond that, the term “directly affect the electrical state” is not sufficiently descriptive in our view. ANY destroyed subsystem necessarily affects the electrical state of the BES, so we don’t think this provides the degree of clarity needed to classify the applicable subsystems.
MWDSC	Disagree	Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding the adjective "interconnected" before the term BES under each bullet. For example, "directly affect the electrical state or the capability of the interconnected BES;" Also, need more specific criteria such as in Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Disagree	Optional definition: A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Disagree	The wording in the definition that states "directly affect" is too ambiguous to apply this criteria. Suggested wording for bullet #1 is " results in a violation of the Transmission Operator's operating criteria." Suggested wording for bullet #3, first sub-bullet is "results in a violation of the Transmission Operator's planning criteria."
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for “BES Impact” such as “BES subsystems that if destroyed, degraded, or otherwise

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines provided in Attachment 1 of this Standard." Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.
BPA Trans	Disagree	Some of our comments for High BES Impact are applicable and are repeated here: 1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this makes sense, but: "BES Cyber Systems need to be "secure" not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-00204 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", etc. In particular, what is, and how long is a "planning time frame"? 3. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is "destroyed, degraded or otherwise rendered unavailable." But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of "Subsystems whose destruction, degradation, or lack of availability could lead to …" The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. Additionally, 4. The verb "affect" is too broad. The Standard does not state that the effect must be harmful. Even if we assume that what is really meant is "affect adversely", we need to define how much is enough. For example; if a print server generates weekly summary reports, then its absence would directly and adversely affect the "ability to monitor… the BES". That would erroneously make it a Medium BES impact. Note that FIPS-199 uses "significant adverse effect" for Moderate Impact, which is the equivalent of Medium Impact in this standard. Question, Why not use "Moderate Impact", instead of "Medium"? FIPS-199 is required for use by Federal agencies and is

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		commonly used elsewhere. It may be sensible to use the same terminology. We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
Allegheny Energy		Medium BES Impact • in a planning time frame, under emergency, abnormal, or restorative conditions, - directly affect the electrical state or the capability of the BES; or - directly affect the ability to effectively monitor and control the BES. "Planning time frame" needs to be better defined
KCPL	Disagree	This is too broad. There will always be a "tipping" point of generation and transmission outages, that, when crossed, yields an unreliable and undesirable operating condition. As an example, any combination of generating facilities within the Eastern interconnect that totals half of the generation meeting load demand, if removed from service, would be devastating to the operation of the BES. The way this is written, all generating facilities that was not included as HIGH would have to be included as a MEDIUM. The same illustration could be used for transmission facilities. In addition, placing the burden of establishing the loss of a facility or group of facilities on the Reliability Coordinators and the reliability impact is a concern as they do not have the resources to manage the likely flood of requests and endless operating configurations that would result from Registered Entities seeking relief from this CIP Standard. If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	See comments for 1.g above.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If a new definition is created, the scope should be limited to "direct" causes and exclude "in the planning time frame." Planning timeframe is vague and varies. As proposed, it cannot be consistently implemented or fairly audited. The standard should address the current rating and impact, not a potential future impact.
CPG	Disagree	This definition takes into account restorative conditions, which are included under the term High BES Impact.
Santee Cooper	Disagree	See comments above, once you rework High BES Impact, the Medium and Low will change as well.
OGE	Disagree	• The terminology is too vague. Any line outage would affect the capability of the BES. • What is meant by the term "electrical state"? Is there a definition for that? What is meant by the term "capability"?

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Is there a definition for that? • OPTIONS: A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES. A post single contingency state in which an additional single contingency may require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES. (N-2?)
Oncor	Disagree	The enforceable definition of Medium BES Impact is actually set by CIP-002 - Attachment 1. Remove from Definition of Terms section.
PPL Supply	Disagree	Comments: Agree with EEI Comments.
St. George	Agree	
NGRID	Disagree	Please elaborate on “electrical state or capability of the BES”. National Grid also recommends considering only bullet 2 – directly affect the ability to effectively monitor and control the BES Reference to BES Cyber system should be made since the Transmission/Generation subsystems will be degraded or destroyed through BES Cyber System (intent of the standard). Also, it is recommended to consider an alternate phrase/word to “destroyed/degraded” as they are generally referred to a physical means of compromise. “BES Subsystems have Medium BES Impact if, when “compromised” through its BES Cyber Systems, they could:…” If the SDT wants to keep this definition then they need to provide more clarity as to which BES Cyber Systems will be included in this category and What are the parameters to determine if a BES Cyber System could directly affect the electrical state or capability of the BES?
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1.
FE	Disagree	We do not support a review/classification of Medium BES Impact threats and therefore disagree with the inclusion of this definition. In addition, this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES".
TECO	Disagree	The amended Attachment 1 categorization definition (see EEI comments) should be used in place of this, as it is more clearly defined. If that cannot be accomplished, references to the “planning time frame” should be removed.
CECD	Agree	Agreement with the definition is based on the registered entity having the independence to define its BES subsystems.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.
GTC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Xcel	Disagree	Comments: See 1.h. In general, we believe the Attachment defines Low, Medium and High and these should be removed from the reference section.
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 g, 1i should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. We feel that the bullet, “directly affect the electrical state or the capability of the BES;” should be removed. The statement is too broad. This also applies to the next to last bullet. Please clarify what is meant by planning time frame? Also, please note response to Q3.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Same as previous (Regarding “High BES Impact” and “Medium BES Impact” references to the “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. Consider striking references to “planning time frame” and replace with “based on analysis of real-time operating conditions.”)
TAPS		See TAPS response to Question 1.a.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Allegheny Power	Disagree	AP believes that the current written definition for medium impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations.
FMPA	Disagree	The definition of Medium Impact is too nebulous and ambiguous. If a transducer goes out of calibration, is that enough to "directly affect the ability to effectively monitor"? We hope that is not the intent of the SDT. Criteria needs to be associated with this definition to make it useful. This is done in the criteria of Attachment 1, so, really, the true definition of Medium BES Impact is in the Criteria of Attachment 1. To add clarity, FMPA suggests incorporating the concept of being dangerously close to an Adverse Reliability Impact, e.g., only a single contingency away, as determining whether a cyber system has medium impact. FMPA suggests: "BES Cyber Systems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could cause a post-contingency system state in which an additional single contingency is likely to result in an Adverse Reliability Impact to the BES, or could hinder restoration efforts"
Duke	Disagree	This definition is not needed because Attachment 1 of the standard describes Medium BES Impact in great detail.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
IESO	Disagree	Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we've got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): a. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. b. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined according to studies or other criteria determined by the RC.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		c. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring compliance.
Manitoba 2	Disagree	This definition very closely resembles the Risk Factors defined in the NERC Reliability Standards Development Procedure, which are used to develop Violation Risk Factors (VRFs), which is redundant, and is not consistent with the impact criteria described in Attachment 1. The definition "Medium BES Impact" should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. It is unclear what is meant by "in a planning time frame" and this point should be removed. The standard is limited to systems that are already in-service. Please define emergency, abnormal, or restorative conditions. Please define "electrical state or capability" of the BES. As currently written, BES Subsystems which have a High BES Impact would also be categorized as Medium BES Impact. Please include a statement indicating that the Medium BES Impact is exclusive of the High BES Impact. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	The phrases "directly affect", "electrical state" and "effectively monitor" does not convey sufficient clarity for entities to properly identify BES Subsystem which should fall into this category. We offer the following three options for the SDT to consider: 1. Delete this classification and keep only the "High" and "Low" classifications. 2. Provide more specificity to the term in order for entities to understand what is the potential impact of facilities classified as "Medium". 3. Do not define the term Medium BES Impact but identify those facilities that fall under this classification level. (Allow entities to use the same engineering assessment identified for "High BES Impact" to determine if the facilities should be moved to either "high" or "Low". Options 1: This option allows the team to focus on those BES Cyber Systems that truly have a high impact on the BES. Option 2: If the SDT wants to keep this definition then they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could directly affect the electrical state or capability of the BES?

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.h. Comment (Response page 12)</th></tr>
<tr><td></td><td></td><td>- Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
- See our comments under High BES Impact for the phrase “under emergency, abnormal, or restorative conditions”.
Option 3: This would eliminate the need for the SDT to define Medium BES Impact and allow entities the options to use an engineering assessment to either raise or lower those BES Cyber Systems that have been identified in Attachment 1.
Example: If an entity could demonstrate through an engineering assessment that a facility identified as Medium BES Impact would not cause instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies) then that facility could be identified as “Low”.
(Please see our comment to question 1e)</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="8">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.h. Comment (Response page 12)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Same comments regarding the third bullet as mentioned in 1.g (the complexity associated with the flexibility in cranking that a restoration plan must address due to the varying scenarios that could occur which makes it difficult to determine one or two critical paths). It is unclear what "affect" means in all three bullets. The loss of functionality is planned for per the Reliability Standards so it is unclear if this deems all diversified BES Subsystems that are established to meet this intent must be treated as Medium or just the "backup" BES Subsystem.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The Standard and Attachment 1 both define what constitutes a Medium BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a Medium BES Impact.</td></tr>
<tr><td>ERCOT</td><td>Disagree</td><td>ERCOT ISO supports Midwest ISO comments.
Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706.
The third bullet of the definition is largely redundant to the first two bullets and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the</td></tr>
</table>

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		standards and how to make new systems compliant upon installation. In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". This is not reasonable and this definition needs to be revised significantly. Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
PacifiCorp	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES Subsystems that may have a high impact in the planning time frame. The standard should address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The Medium BES Impact definition appears to mimic the definition of a Medium Violation Risk Factor. We question why there is a need to consider "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation.
PEPCO	Disagree	The current definition for Medium BES Impact BES systems does not bring sufficient clarity for determining the appropriate category. See suggestion under High BES Impact.
NEI	Disagree	A) We do not support a review/classification of Medium BES Impact threats and therefore disagree with the inclusion of this definition. In addition, this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". B) It is recommended that Attachment 1 be used to provide an adequate definition, and that the Glossary be point to the Attachment. C) If the definition is to be kept, provide clarification for the term "directly affect". D) Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		starting list is developed in the Appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not:

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Summary Consideration:

Organization	Yes or No	Question 1.i. Comment (Response page 13)
Progress Energy	Disagree	Either change to No Impact (and only classify High and Medium BES Impact) or remove all bullets under Low BES Impact and add "…could not: • Directly and immediately cause or create: - BES instability; and/or - violation of an IROL • Directly affect the ability to effectively monitor and control the BES."
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a "Low BES Impact (Reliability)" and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with "Low BES Impact" criteria and then add a "No BES Impact" category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for "Low BES Impact" BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.
GSOC/OPC	Disagree	We suggest replacing this definition with something consistent with Attachment 1.
Hayden	Agree	
SDGE	Disagree	Are the bullet items OR (mutually exclusive) or AND? Same comment applies on the need for clarity and definition of

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		"directly affect the electrical state or capability of the BES". What does "unacceptable risk" mean, when does it become "acceptable risk"? We propose eliminating the phrase "directly affects the electrical state" – it is ambiguous and includes virtually every scenario. If "BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not: • directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures, etc." We propose this classification be changed to "No BES impact" instead of "Low BE impact".
APPA	Disagree	APPA Task Force Suggested Definition: Low BES Impact: BES Cyber Systems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, are unlikely to cause a post-contingency system state that will result in an Adverse Reliability Impact to the BES, but is still considered necessary for the reliable functioning of the BES.
Consumers	Disagree	As proposed, this lumps all other BES Subsystems into Low Impact, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule or non-existent its potential impact. What benefit is derived from identifying and placing thousands of devices in a listing of low impact? In addition, if NERC later decides that there is even one requirement in the low impact category, the compliance evidence burden placed on REs will be extremely onerous. As such, the majority of a RE's compliance tracking and evidence gathering efforts would be spent on the low impact category and critical systems will simply be part of the mix, but not receive the attention due. As mentioned earlier, this should simply be renamed as No Impact and although a listing of the subsystems may be warranted, no listing of corresponding cyber systems is justified nor should be required for this category.
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be "merely guidelines" and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the "planning time frame" which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves. Finally, the word "hinder", which is ambiguous and subjective, should be changed to "prevent".
MPPA	Disagree	This should have a similar quantifying reference as the first two. It recommended that the ", not categorized as High or Medium BES Impact," be inserted into the first line such that it reads as follows: "…BES Subsystems, not categorized as

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		High or Medium BES Impact, have Low BES Impact if…”
Central Lincoln	Disagree	No distinction is made between systems that have low impact and between systems that have no impact. While systems that have no impact should not have been included in the BES in the first place, the uncertainty around the BES definition has caused registered entities and regional entities to include such systems in the BES. This could potentially force entities unnecessarily into compliance with CIP-003 through 009. On the second bullet: Restoration from what condition? If left to overreaching regional entities, any system that could delay restoration following a small local outage will put that system in the high BES impact category even if it is not part of the BES.
NERC	Disagree	Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as “contribute to”, and “create an unacceptable risk”. More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems
Dominion	Disagree	See comment to 1.h. above.
Encari	Agree	
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the current definition for low impact BES systems does not bring sufficient clarity to the classification process. SCE urges the Drafting Team to distinguish between those systems having a low impact and those having no impact. SCE recommends creating a “Not Applicable” category for assets that may reside in an Electronic or Physical Security Perimeter, but which have no impact on the BES. SCE also requests clarification on certain ambiguous terms. For example, the term “hinder” is ambiguous and overly broad, as it is not defined by any reference to a duration or degree of impact. The term “unacceptable risk” is also ambiguous, as it is unclear which party’s assessment of risk will be respected. It is unclear what the meaning of “electrical state” is, as that term is not defined in the NERC Glossary of terms.
USBR	Disagree	The term is defined as having no impact yet the term is called "Low Impact". The definition is not needed as there is no impact to the BES. The term can be eliminated without loss to the standard.
Dyonyx	Disagree	The term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a "Low BES Impact (Reliability)" and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with "Low BES Impact" criteria and then add a "No BES Impact" category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for "Low BES Impact" BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.
Westar	Disagree	There should be a No Impact category instead of a Low BES Impact category. Entities would then identify High and Medium Impact assets which would then require a certain set of controls. All other assets would be in the No Impact category and no controls would be necessary.
Green Country	Disagree	A single event that will not cause an Adverse Reliability Impact to the BES
Oregon PUC	Disagree	Having three impact levels is too complex and confusing for utilities and operators. We further do not see the benefit-cost need for this lower level. Also, it is difficult to prove a negative outcome as indicated by the term "they could not". We recommend there only be two BES impact levels at most. To have three levels will only cause unnecessary confusion to the industry and introduce greater opportunity for different interpretations by responsible and enforcing entities.
Manitoba 1	Agree	You probably have to also define what they could do (only defined could not). Need clarification on what is needed by third party review to make acceptable.
Portland GE	Disagree	It is unclear how an entity would be able to "prove the negative" in order to demonstrate that a BES subsystem "could not" affect the BES in the manner described in the proposed definition. In addition, it is not clear whether this requirement/definition or the requirements in Attachment 1 are the governing provisions.
PSEG	Disagree	Comment #1: Ultimately we do not believe that there is a need for a definition of "Low BES Impact" nor for a classification of Transmission Subsystem that would fall into this category. We believe that entities should only have to identify facilities that qualify as "High BES Impact" or "Medium BES Impact" and therefore have to comply with CIP-003 – 009 reliability standards. As the definition for "Low BES Impact" explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. As NERC looks towards Results-base requirements, nothing would be gained by requiring entities to list subsystems that fall under this category. We do not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any subsystem that does not fall into the "High" or "Medium" buckets will by default fall into the "Low" bucket. Comment #2: Does the phrase "hinder restoration" refer to a time delay for restoration? In other words an entity can

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		restore their system but the cyber attack may cause some time delay for the restoration effort to be completed. Comment #3: We believe that if the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES? - Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. In addition, Wisconsin Electric Power Company feels low impact subsystems should not be considered in this standard. This category includes systems that would have zero risk to the BES and as currently defined would create a large work effort to categorize and maintain with little value eliminating risk to the BES.
Idaho Power	Agree	
SOCO	Disagree	There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each and let those be the definitions and not have them up front at all. The standard currently has criteria for High and Medium impacts and lumps all other BES Subsystems into Low, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule its potential impact. If there is even one requirement in the low impact category and that category is auditable and enforceable, the compliance evidence burden placed on entities will be onerous. Since there is no bottom to this standard and low is the 'everything else' category, every cyber system in the BES of North America will be on the list and in scope. There may be tens of thousands of systems per entity (would not each relay be a 'cyber system'?). The majority of your compliance tracking and evidence gathering will be on the lowest impact, but orders of magnitude more numerous cyber systems. If the TFE process also applies to these millions of systems continent-wide we are creating an unmanageable bureaucracy. The standard needs minimum criteria. Since the Low impact category is simply a catchall, we propose there be no requirements for low. This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions. General section comment: Insert a diagram to clarify the delineation of the defined terms as related to each other.
DTE	Disagree	The intention of this category seems to be to capture all BES subsystems that are not High or Medium BES Impact. Changing the language from a qualifier to a disqualifier could cause confusion. To keep the language in parallel with High and Medium BES Impact, we suggest changing the definition as follows: Low BES Impact — BES Subsystems not

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		classified as High BES Impact or Medium BES Impact. If the drafting team does not agree with our version of the definition, we are concerned that the term “unacceptable risk” is reintroducing the “acceptance of risk” concept that was removed from previous versions.
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a “No BES Impact” should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	The term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	The criteria for "low" impact seems to us to represent *no* impact, which we presume is not the SDT's intention. We recommend this definition be revisited.
Flathead	Disagree	Low impact assets by definition are not critical. It defies logic that they would be included as critical and subject to CIP-003 through CIP-009 just like the actually critical assets.
E ON	Disagree	E ON U.S. sees no need for this category. Inclusion of this category establishes the necessity of inventorying and assessing the BES impact of every conceivable BES Subsystem. Given that by definition BES subsystems falling into

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		this category have no impact on overall BES reliability, E ON U.S. questions the need for such an expansive exercise and use of limited resources
Carthage	Agree	
WECC	Disagree	If this is could not impact then this should be “no impact” not low impact.
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a and 1.h. This appears to be a definition of “no BES impact” and therefore should not be listed as “Low BES impact”. BES systems that do “not” cause any of the impacts listed should not require security measures to be employed.
LCRA	Agree	1. The “Low BES Impact” category must result in very few security controls. 2. The phrase “directly affect” should be changed to “directly and adversely affect”. The original phrase is too broad.
FRCC	Disagree	See comments to question 1.h
NIPSCO	Disagree	We do not believe that there is a need for a definition of “Low BES Impact”. As the definition for “Low BES Impact” explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. Suggestion: Eliminate the proposed category or review and revise the criteria of a Low BES impact asset.
ConEd	Agree	
EEI	Disagree	EEI believes that the current written definition for low impact BES systems does not bring sufficient clarity for determining the appropriate category. Use of phrase: “BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not:…” creates a nearly impossible burden of proof. It is difficult or impossible to ‘prove’ or demonstrate a system has these properties. Moreover, terms such as ‘hinder’ are vague and open to wide interpretation. In addition, the state of the electrical system is affected “directly” by normal events, such as customer load. Finally, we do not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any subsystem that does not fall into the “High” or “Medium” buckets will by default fall into the “Low” bucket.
O&R	Agree	
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of Medium BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "Low BES Impact". If it is necessary that all BES Subsystems need to be in one of

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		the three categories then Low BES impact should be defined as all BES Subsystems that are not included in High BES Impact or Medium BES Impact. However, we believe a fourth category should be added which is “No BES Impact”, for example radial facilities. If this suggestion is adopted then the Low BES Impact offered should be revised accordingly, e.g. loss of load less than 100 MW.
Black Hills	Disagree	What proof is necessary to justify a "could not" declaration? Other common term questions as in previous sections.
TNMP	Disagree	Comments on High BES Impact are equally applicable to this definition.
NVEnergy	Disagree	We understand the concept behind this definition, but note that as written, it carries the same degree of vagueness that we object to in the High and Medium categories. Also, we wish to note that if the above bullets are true (no unacceptable risk to BES, no hindrance of restoration, no effect on capability nor ability to monitor the BES), then it is unreasonable to assign even a “Low Impact” to the subsystems. Perhaps a “No Impact” category is in order.
MWDSC	Disagree	Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding a bullet to the term "Low BES Impact" such as…. "..not: create an Adverse Reliability Impact (as defined in NERC Glossary) of any interconnected BES". Also, if an engineering evaluation demonstrates no Adverse Reliability Impact of any interconnected BES, recommend adding a separate category such as "No BES Impact" or a subcategory under "Low BES Impact" with limited application of unknown security requirements in CIP-003 through CIP-009.
Empire	Disagree	Optional Definition: A single event that will not cause an Adverse Reliability Impact to the BES.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Agree	
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for “BES Impact” such as “BES subsystems that if destroyed, degraded, or otherwise rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines provided in Attachment 1 of this Standard.” Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
BPA Trans	Disagree	Some of our comments for High BES Impact are applicable and are repeated here: 1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this makes sense, but: "BES Cyber Systems need to be “secure” not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-00204 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", “unacceptable risk,” “hinder restoration,” etc. In particular, what is, and how long is a "planning time frame"? 3. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is “destroyed, degraded or otherwise rendered unavailable.” But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of “Subsystems whose destruction, degradation, or lack of availability could lead to …” The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. Additionally, 4. It appears that this definition is too vague. Recommend the last two bullets read "directly and adversely affect…" Any adverse affect, no matter how small, would cause the Subsystem to have at least a Medium Impact. This is really a definition of "No Impact", not "Low Impact". 5. Bullet 2 should read: "directly hinder restoration of the BES to a normal condition." "Directly" is needed in this instance to make it clear that indirect affects are outside the scope of the definition. "Of the BES" is again needed so we know what the reference is. 6. Are these four bullets joined by "and" or "or"? The intent would seem to be "and": if the Subsystem could do any one of the things listed in the bullets, it could not be Low impact. However, since the conjunction is not specified, one could argue that a system that could do 3 of the 4 could still be Low Impact. Again, the FIPS-199 approach could be useful. It limits "Low Impact" to systems that would have a "limited adverse

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		effect". This is much more realistic. Note also that FIPS-199 ignores systems that can have no effect. This is appropriate. We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
CCG	Disagree	CCG does not support the definition of "Low BES Impact" nor the concept of categorizing all assets into three groups, all of which will require some level of protection. Categorizing BES assets as "Low Impact" when the definition specifically states these assets "could not" have any impact is entirely inappropriate. This exceeds what is needed for reliability.
Allegheny Energy	Agree	
KCPL	Disagree	If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	See comments for 1.g above.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset.
CPG	Disagree	This definition should just state that it includes all other BES Subsystems not defined as High or Medium BES Impact. Since this group of subsystems does not fall into the High or Medium Impact levels, the name of this group should be changed to "No BES Impact."
Santee Cooper	Disagree	See comment to Medium BES Impact.
OGE	Disagree	• The terminology is too vague. What is "an unacceptable risk"? How much of an impact must occur before something has "directly affected" the BES? • "Normal condition" needs to be defined in this context. • OPTION: A single event that will not cause an Adverse Reliability Impact to the BES. A post contingency system state that will not cause an Adverse Reliability Impact to the BES.
Oncor	Disagree	The enforceable definition of Low BES Impact is actually set by CIP-002 - Attachment 1. The descriptions of what "Low BES Impact" is not should be included in Attachment 1.
PPL Supply	Disagree	Comments: Agree with EEI Comments.
St. George	Disagree	As a small municipality, we applaud the draft team for dealing with the over-simplistic classification of an asset as Critical or Non-Critical. The proposed standard takes two classifications (Critical and Non-Critical) and makes three (High, Medium, and Low). We are deeply concerned that three classifications are not sufficient to represent the true nature of

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		the BES. At minimum another classification should be added: Minimal. This would be for Generation Subsystems below 200 MVA and transmission below 150 kV in the Eastern and Western Interconnections. Low would then be for Generation Subsystems of 200 – 1,000 MVA and transmission of 150 – 200 kV in the Eastern and Western Interconnections. The Minimal classification assets would then be exempt from CIP-003 through CIP-009 in the same way Non-Critical assets are currently.
NGRID	Disagree	It is still unclear if "low BES Impact" systems will require any security controls and will be clear only when CIP-03 through CIP-09 are released. If they do not require any security controls (which currently looks to be the case), it is recommended to delete this definition. Nothing will be gained by maintaining this list especially as we move towards Results based Standards. If the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the parameters to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES?
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1. MGE does not support the three level approach. MGE would support a four level approach that has the addition of a "No BES Impact" category. This category would contain cyber assets contained in a Registered Entity's UFLS program. The purpose of the UFLS program is to provide a last resort for system preservation. It is not defined in the UFLS Standards that the UFLS program is to maintain BES stability, but that is why there is a UFLS program. By not having a No BES Impact category, the SDT is not giving a bright-line solution for those entities who are only DP's with an UFLS program, etc. When given a Bright-line solution, the entity will see that that there are two sides. The three category has all cyber assets on one side. The No Bes Impact category will give the SDT and the entire industry the solution to this issue by stating what cyber assets impact the BES and which don't (No BES Impact).
FE	Disagree	We do not support a review/classification of Low BES Impact threats and therefore disagree with the inclusion of this definition. If it remains, then Low BES Impact Subsystems should require minimal or no security controls since by definition the Low BES Impact would NOT contribute to BES problems.
TECO	Disagree	We support EEI's comments and offer the following additional suggestions. The term "unacceptable risk" needs to be more clearly defined. Additionally we are concerned with the existence of VSLs that relate to subsystems that by definition have no impact.
CECD	Disagree	If a BES Subsystem cannot directly affect the electrical state or capability of the BES or directly affect the ability to effectively monitor and control the BES the Registered Entity should be able to state that there is No BES Impact.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.
GTC	Disagree	We suggest replacing this definition with something consistent with Attachment 1.
Xcel	Disagree	See 1.h. In general, we believe the Attachment defines Low, Medium and High and these should be removed from the reference section.
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 g, 1 h should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. 1st bullet….”unacceptable risk” not well defined. It is vague and should be linked to NERC transmission planning standards. “Cascading Sequence of failures” is not clearly defined We feel that the bullet, “directly affect the electrical state or the capability of the BES;” should be removed. The statement is too broad. In the phrase, “Or could hinder restoration to normal condition”, “normal condition” is not clearly defined. Also, please note response to Q3. We believe that there should be a “No Impact” category. This could be accomplished by eliminating the “Medium Impact” category and redefining “Low Impact” with the current “Medium Impact” definition as modified with our comments in 1.i.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although we appreciate the idea of categorizing an impact as low, we do not think it provides any additional benefit to the BES since most of the key points have been captured in the high and medium.
TAPS	Disagree	The proposed “low impact” category, as currently defined, includes subsystems--and, therefore, cyber systems--that have no impact on the bulk electric system. Cyber systems that have no potential impact on the reliability of the BES should not be subject to security controls. Nor should such systems be subject to NERC's registration and compliance regimen. By capturing such facilities, therefore, the proposed standard would impose significant costs on responsible entities and Regional Entities with no commensurate benefit to reliability. The lack of impact on the BES also puts the statutory basis for such coverage into question. To achieve the standard’s cyber security purposes in a cost effective and rational manner, consistent with Section 215, the identification of cyber assets should be restricted to those facilities that have a meaningful potential impact on the BES; cyber assets with no potential impact on reliability should be classified in a fourth, “No Impact” tier. This approach is consistent with the statement of Gerry Cauley in his planned comments to the MRC on Monday, February 15 (available at http://www.nerc.com/docs/mrc/agenda_items/AgendaItem_6.pdf) that there should be “minimum bright-line criteria for identification of critical bulk power system assets.” The existence of a “bright

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		line" necessarily entails the exclusion of systems, such as those with no impact on the BES, that fall below the "bright line."
Allegheny Power	Disagree	AP believes that the current written definition for low impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Attachment 1 to make such determinations.
FMPA	Disagree	See comments to Medium BES Impact concerning ambiguous definition FMPA suggests a less ambiguous definition of: "BES Cyber Systems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, are unlikely to cause a post-contingency system state that will result in an Adverse Reliability Impact to the BES, but is still considered important to the reliable functioning of the BES." Or possibly more clarity by specifying "more than a single contingency away" from an Adverse Reliability Impact. Also, it is difficult to develop an opinion on Low BES Impact without understanding what requirements, if any, will be imposed on Cyber Systems with Low BES Impact in standards CIP-003 through CIP-009. We cannot agree with the definition until these requirements, if any, are made clear. We believe strongly that there is no need to regulate cyber security of Low BES Impact Cyber Systems, and any requirements placed on Low BES Impact Cyber Systems would be against the intent of the EPAct of 2005, which was specifically geared towards maintaining "reliable operations" to prevent "instability, uncontrolled separation, or cascading", which is already captured in High BES Impact. If the SDT believes that some requirements are necessary for the Low BES Impact Cyber Systems, such requirements should be programmatic in nature and not Cyber System specific, such as training. Any Cyber System specific requirements for Low BES Impact Cyber Systems would be unduly burdensome to the Entities with no value to BES reliability.
Duke	Disagree	This definition is not needed because Attachment 1 of the standard clearly explains that all BES Subsystems which are not High BES Impact or Medium BES Impact are Low BES Impact.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	We suggest replacing this definition with something consistent with Attachment 1.
IESO	Agree	The term "risk" is misused in the phrase "unacceptable risk of". the term should refer to the "unacceptable likelihood of" Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we've got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): a. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. b. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		according to studies or other criteria determined by the RC. c. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring compliance.
Manitoba 2	Disagree	The definition "Low BES Impact" should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. By the definition, these BES Subsystems do not have an impact on the reliability of the BES, and therefore should belong in a "No BES Impact" category. If a "No BES Impact" category is not provided, the controls for the Low BES Impact category should not be auditable. There needs to be some consideration of acceptance of risk for minimal reliability benefit. A categorization level where no mandated security controls are required should be included. Previous comments regarding a "No Impact" category by multiple entities responding to the concept paper, including Manitoba Hydro, were not incorporated into this latest version of CIP-002. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA		OMPA suggests the addition of an additional tier for "no BES impact".
ATC	Disagree	Ultimately ATC does not believe that there is a need for a definition of "Low BES Impact" nor for a classification of Transmission Subsystem that would fall into this category. We believe that entities should only have to identify facilities that qualify as "High BES Impact" or "Medium BES Impact" and therefore have to comply with CIP-003 – 009 reliability standards. As the definition for "Low BES Impact" explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. As NERC looks towards Results-base requirements would is being gained by requiring entities to list subsystems that fall under this category. If the SDT rejects our above recommendation: 1. ATC does not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any subsystem that does not fall into the "High" or "Medium" buckets will by default fall into the "Low" bucket. If the SDT does not agree with our suggestion to delete this definition then we believe that they need to address the following questions: 2. Does the phrase "hinder restoration" refer to a time delay for restoration? In other words an entity can restore their

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.i. Comment (Response page 13)</th></tr>
<tr><td></td><td></td><td>system but the cyber attack may cause some time delay for the restoration effort. (The delay will result in X amount of hours over planned activities)
Lastly ATC believe
2. If the SDT wants to keep this definition then they need to provide more clarity as to what BES Cyber Systems will be included in this category.
- What are the qualifiers to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES?
- Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
(Please see our comment to question 1e)</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><td>Physical Perimeter</td><td>Data Encryption</td><td>Antivirus</td><td>OS Patches</td><td>Intrusion Detection</td><td>Account Passwords</td><td>Firewall</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.i. Comment (Response page 13)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>It appears this is the catch all bucket for all remaining BES Subsystems. It is unclear whether an entity would be required to prove that a BES Subsystem "could not" do as bulleted which seems of little value. It is unclear why every BES Subsystem must be categorized at all instead of focusing purely on that which is "high" and "medium". The subsequent need (R1) to update and maintain lists as a result of this is labor intensive and because CIP-003 through CIP-009 modifications for version 4 have not been provided it is difficult to determine the value in this exercise.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The Standard and Attachment 1 both define what constitutes a Low BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a Low BES Impact.</td></tr>
<tr><td>ERCOT</td><td>Disagree</td><td>ERCOT ISO supports Midwest ISO comments.
Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706.
Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a</td></tr>
</table>

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		"Low BES Impact (Reliability)" and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with "Low BES Impact" criteria and then add a "No BES Impact" category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for "Low BES Impact" BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.
PacifiCorp	Disagree	- Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES Subsystems that may have a high impact in the planning time frame. The standard should address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The Low BES Impact definition appears to mimic the definition of a Low Violation Risk Factor. We question why there is a need to consider "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation
PEPCO	Disagree	The current definition for Low BES Impact does not bring sufficient clarity for determining the appropriate category. Use of phrase: BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not… creates a nearly impossible burden of proof. It is difficult or impossible to prove or demonstrate a system has these properties. Moreover, terms such as hinder are vague and open to wide interpretation. In addition, the state of the electrical system is affected directly by normal events, such as customer demand. See suggestion under High BES Impact.
NEI	Disagree	A) NEI does not support a review/classification of Low BES Impact threats and therefore disagree with the inclusion of this definition. If it remains, then Low BES Impact Subsystems should require minimal or no security controls since by definition the Low BES Impact would NOT contribute to BES problems. B) Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the Appendix). While the current "one size fits all" approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Organization	Yes or No	Question 2 Comment (Response page 14)
Progress Energy	Disagree	To provide additional clarity, CIP standards should only address real-time cyber operations. See also the Question 1 comments above.
Dynegy	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems as critical and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets
GSOC/OPC	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Hayden	Disagree	CIP-002-4 overly complicates the approach delineated in CIP-002 (earlier versions). In the earlier versions it was a straightforward approach where the Registered Entity identified its Critical Assets (i.e., those assets that could affect the BES) and then you identified the supporting Cyber Assets and then the Critical Cyber Assets. The approach in this newly revised standard takes this systematic approach and appears to complicate the process with new terms and definitions that I am not certain help the Registered Entity better understand the process. Attachment 1 is helpful in providing more specifics on what constitutes a Critical Asset so why not just use Attachment 1 to say that if you have an asset and it satisfies these requirements it is now a Critical Asset?

Organization	Yes or No	Question 2 Comment (Response page 14)
SDGE	Disagree	We agree in principle with the purpose statement, but in several locations throughout the Standard the drafting team uses ambiguous language that needs to be easier to understand and interpret. Examples include: • Identifying BES Cyber Systems is plausible, given the language in this draft. However, the categorization of BES Systems given the existing language is likely to result in multiple interpretations and inconsistencies throughout the industry. • Because the “High BES impact” and “Medium BES impact” definitions are so close to each other, security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES could require entities to implement the same or very similar controls for the “High” and “Medium” impact classes to ensure compliance. • How will certain CIP-003 through CIP-009 requirements be treated for the three BES impact classes such as training, vulnerability assessments, PRAs, access controls, etc.? Again, we propose having just two impact classes to help make the implementation and management of these Standards easier.
APPA	Disagree	APPA Task Force Comments: The addition of new terms of "subsystem" and "functions" add complexity and confusion. How are these new functions related to the Functional Model, for instance? The real focus ought to be on the worst case contingencies / scenarios that can be caused by malicious manipulation of a cyber system. Such a focus bypasses the need to create new terms such as subsystems and functions.
Consumers	Disagree	We do not believe the proposal accomplishes the goal because the cyber systems simply inherit the categorization of the BES Subsystem. To apply appropriate cyber security controls, the SDT needs to create a means so that cyber systems are categorized separately from the subsystems. As in previous versions of the standard, first address the critical nature of the subsystems (assets) then address how critical (or not) are the associated cyber systems. The requirements for protecting these assets (via CIP-003 >> CIP-009) should then vary based on how critical the cyber system is to the functioning of the subsystem. Note that this means that ALL cyber systems would not need to be categorized, but only those that are associated with the critical BES Subsystems. Much like the previous revisions of CIP-002, a “critical” evaluation/test needs to first be passed before further investigating the cyber assets. The exception would be those systems (subsystems according to the new definition), such as SCADA, but only if that (or similar systems) have external routable protocol, networking, or dial-up connectivity. If FERC wants to issue one order to include all CIP Version 4 standards, they should hold the vote on CIP-002-4 through CIP-009-4 at the same time after review and comments have been made on all eight standards. The industry should have an understanding of all the CIP version 4 standards before voting.
NPCC	Agree	

Organization	Yes or No	Question 2 Comment (Response page 14)
SWPA	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems and to require protection. The drafting team should establish bright lines for criteria which could satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.
MPPA	Disagree	The standard, in its current form, does not accomplish its purpose. The standard needs to quantify the differences of High, Medium, and Low BES Impact definitions in a clearer manner. It needs to provide consistency between the R1 VSL, and the R2 VSL.
Central Lincoln	Disagree	See 1.i. above.
NERC	Disagree	The standard appears to draw an implied distinction in the purpose statement and in the definition of BES Cyber System by using the language about functions "critical to the reliable operation of the BES". While Attachment 2 defines the eight BES critical functions, we create an unneeded distinction by using the word "critical". Critical is not defined nor is an understood framework available for use. The team can achieve the same goal by changing the purpose statement and Attachment 2 to eliminate the use of "critical" and replace it with "necessary", a word that is straight forward in its definition and that does not carry the existing concerns.
Dominion	Disagree	CIP-002-4 does not accomplish the objective because of the uncertainty it introduces. Clear, concise and well-defined statements and terms are needed to satisfy the stated objective.
Encari	Agree	
US ACE – NW	Agree	
SCE	Disagree	SCE recommends that the Standards Drafting Team put forward a single package of proposed standards that includes both the proposed standards for BES Cyber System Categorization, as well as the associated control standards. This would allow the industry to perform an overall impact analysis of the proposed standards and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of the associated controls in CIP-003 through CIP-009. SCE's recommendation is based on the fact that it is impossible to judge the proposed purpose behind CIP-002-4 without considering the types of controls that will follow from categorizing BES Cyber Systems as "low, medium or high" impact systems. The nature of controls will vary vastly between what is high impact electrical and cyber versus simply high impact electrical, and the industry is not in a position to make any judgments about this stated purpose until it sees the type of controls that NERC proposes will support that purpose. Finally, SCE is concerned by the fact that the proposed three levels of categorization for the BES Cyber Systems ignore the great importance of cyber connectivity. For example, an IP routable network type of cyber system will have a different set of vulnerabilities than one that is based on dial-up connectivity. These two channels of electronic access will differ

Organization	Yes or No	Question 2 Comment (Response page 14)
		from a network based on serial protocols. This is concerning to SCE because the technical architecture of a particular network type and the data being communicated on it is amenable only to a select set of security controls. While some security controls are universally applicable they may not offer targeted protection to control systems in a manner where the control is commensurate with the vulnerability.
USBR	Disagree	It is not clear what added value is achieved by categorizing assets or cyber systems other than having an impact. FERC has clearly stated no risk is acceptable. Grading the assets asserts a level of risk. The proposed standard should describe objectives of criteria which the Responsible Entities need to develop to assess BES impacts for either Assets or Cyber Systems. The proposed standard does appear to describe requirements of when the criteria is to be used, which is good. Unfortunately the "criteria" tries to identify elements rather then what the Responsible entity should use to assess the elements. As indicated in the comments and suggested changes for the other sections, the language needs to be clarified.
Dyonyx	Agree	
MISO	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on “functions critical to the reliable operation of the Bulk Electric System (BES)”. Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems as critical and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.
Westar	Disagree	Again, there is a large number of BES assets that have absolutely no Adverse Impact on the BES. There needs to be a No Impact category.
Green Country	Disagree	It clearly is not commensurate since in the situation of NO impact to the BES, the next step the asset up to LOW impact and will require compliance with CIP-003 thru 009 at some level. Which again is not following the Standard Process Manual “Market principals” bullet point #1. It gives an unfair business advantage to regulated utilities to recover costs through rate base.
Oregon PUC	Disagree	CIP-002-4 as proposed is too complex and vague for industry implementation. This is a cornerstone standard that will set the basis for other NERC and regional standards (especially CIP-003 through CIP-009). We believe that clarity, specificity, technical accuracy and relative simplicity are critical for this standard. At the very least we recommend that the Lower BES Impact level be eliminated.
NB Power Gen	Agree	In general I agree that this draft of CIP-002-4 significantly improves identifying and categorizing the BES Cyber Systems that support the functions critical to the reliable operation of the BES. However, as noted in my previous comments, the application of security controls commensurate with the impact should also include the context of threat. The current CIP-002-4 seems to me to change the context to include much more than threats from remote access. If we are protecting against the threat of single or multiple simultaneous remote access to our systems, then we should recognize that lack of

Organization	Yes or No	Question 2 Comment (Response page 14)
		the possibility of such access should be recognized as a secure state that does not require additional security measures other than appropriate change management to ensure no new access is introduced. Otherwise, the full range of CIP standards will be applicable to all cyber systems whether stand alone or not, which is perhaps more of a physical security issue (items of concern are only accessible within the facility).
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree that the proposed CIP-002-4 achieves the stated objective. Cyber systems are not identified and Attachment 1, specifically 1.10, 1.11, 1.12, would require various multiple studies of the subsystems identified because it is unclear as written how widespread an event would have to be to constitute “voltage collapse” or “system collapse." In addition, it is unclear, if the language is intended to get at a very granular level, whether the data is available. There is no way to know whether the controls are “commensurate with the potential impact” without understanding what the full extent of those controls will be for assets that are rated as High, Medium, or Low BES Impact. This standard as proposed is too vague in definition and too complex and burdensome in implementation to justify any perceived marginal enhancement to reliability that may result from the proposed changes. Clarity and specificity that can be uniformly applied across utilities and for auditors is necessary for this standard.
PSEG	Disagree	Comment #1: We believe that the purpose of this standards is to identify those BES Cyber System which are “critical” (i.e. could cause instability, separation or cascading) to the BES. Suggestion: To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) which are “critical” (i.e. could cause instability, separation or cascading) to the Bulk Electric System (BES) as a basis for applying security controls. Comment #2: We believe that the approach utilized makes an effort to categorized BES assets but does not take the same effort to categorize BES Cyber Assets. The BES Cyber Asset now inherits the impact categorization of the BES asset. This again creates a one-size fits all solution for the cyber requirements of the BES Cyber Asset. Comment #3: We believe that if BES system didn’t have external connections, it should not be included as an asset to be protected.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI’s comments regarding this question. We also would like to note that we disagree with the inclusion of cyber assets that utilize a non-routable protocol. These devices do not pose a threat from external attack. In addition, Wisconsin Electric Power Company feels a cyber system is one that has connectivity to a network or the Internet. Devices that may be isolated or stand-a-lone systems where there is no network connectivity should not be considered a cyber system.
Idaho Power	Disagree	The criteria to categorize the cyber systems are too vague and will not provide good guidance to the entities attempting to categorize their cyber assets. If the cyber system supports a function critical to the reliable operation of the BES, haven’t you by default categorized it as critical (high). Why go through the effort to categorize the BES subsystems if the

Organization	Yes or No	Question 2 Comment (Response page 14)
		cyber systems have already been categorized as critical in Attachment 2 if they support one of the listed functions.
SOCO	Agree	The effective date of this Standard should be directly related to the effective dates of all forthcoming daughter standards. The scope of these standards are very extensive, the requirement to categorize all systems within less than 2 years and to maintain this categorization without further active standard requirements presents an unnecessary burden. Consideration should be given to the potentially limited supply of hardware and knowledgeable personnel to the electric and other critical infrastructure industries for compliance with this and other similar regulations.
DTE	Agree	
AEP	Disagree	AEP is interested in the same outcomes as though of the SDT – a secure and reliable Bulk Electric System (BES). In fact, AEP believes that the SDT is headed in the direction, but has not been given enough time to get to the necessary results. AEP is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation (http://www.nerc.com/fileUploads/File/CIP/706-SDT-Webinar-Presentation.pdf) with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low." The resulting table outlines a graduated level for applying cyber security controls to BES Cyber Systems based on risk. BES Cyber Systems that have a low risk should not require the same cyber security controls as BES Cyber Systems that pose a high risk. Ratcheting the risk level to protect nearly everything will inadvertently result in a decline in the reliability of the BES.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	E ON U.S. does not agree that CIP-002-4 accomplishes the intended objective. The definitions are, as noted above, in several instances too expansive and ambiguous. Identification of BES cyber systems becomes an exercise in categorizing every cyber component associated with any operating facility of any type. Also, cyber-systems associated with marketing or other non-operational functions (e.g., planning) are specifically

Organization	Yes or No	Question 2 Comment (Response page 14)
		mentioned as being excluded from consideration in the Categorizing Cyber Systems: An Approach Based on BES Reliability Functions document (page 7) unless they also affect the reliable operation of the BES. These systems are not specifically excluded in the draft standard. E ON U.S. suggests including this specific guidance under one of the existing definitions (e.g., BES Cyber System or High/Medium BES Impact).
Carthage	Agree	
WECC	Disagree	Although NERC has taken a focus on impact based analysis, the definitions are still too open to probability and interpretation in the risk assessment with terms such as “could potentially”, “unacceptable risk”, and “hinder”. If NERC wishes the probability to be considered 100% then all ambiguity and potential for interpretation needs to be removed from definitions.
Entergy	Agree	This is the proper ‘purpose’ of the standard, but the specified required approach to reach this purpose is ill-conceived. Specific recommendations for properly addressing the issues at hand are presented in response to Question 13 below.
CenterPoint	Disagree	Disagree – Setting aside the flaws of the subsystem approach, it is not clear what will be the basis for applying security controls commensurate with potential impact. Therefore, it is not clear whether CIP-002-4 would accomplish any objective.
Ca Cogen	Disagree	As explained above, the concern is with accessibility. Security controls should be applied only to those assets that are vulnerable.
LCRA	Agree	It is very difficult to properly evaluate the revised CIP 002 document without being able to see the rest of the revised standards. While the underlying assumption for categorizing BES Cyber Systems is the need for differing levels of protection, it is unclear how the existing standards CIP 004-009 will be applied to these systems.
NIPSCO	Disagree	We believe that the approach utilized makes an effort to categorize BES assets but does not take the same effort to categorize BES Cyber Assets. The BES Cyber Asset now inherits the impact categorization of the BES asset. This again creates a one-size fits all solution for the cyber requirements of the BES Cyber Asset. Suggestion: Eliminate the BES protection level inheritance. Allow the cyber assets to be evaluated based on the impact to the asset, not based on the impact of the asset to the BES. If this inheritance approach was left as proposed by the SDT, we would need to see how the one size fits all approach is being addressed throughout CIP-003-4 through CIP-009-4.
ConEd	Disagree	Need improved clarity in the definition. Use examples of the common systems and show how they would be categorized. There is too much engineering analysis required to determine if a system belongs in the high or medium category.
EEI	Disagree	EEI is very appreciative of the efforts of the drafting team. In particular, we believe that it is important and appropriate to apply “security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES.”

Organization	Yes or No	Question 2 Comment (Response page 14)
		This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations.
O&R	Disagree	Need improved clarity in the definition. Use examples of the common systems and show how they would be categorized. There is too much engineering analysis required to determine if a system belongs in the high or medium category. NERC should consider that certain entities may have facilities that fall under the BES definition for a given region, but because of their own system's characteristics, do not have an impact on the Interconnected BES. There should be an additional category of NA, as with other NERC Reliability Standards. Since the NERC standards apply as per the entity's registration, the entity would then need to provide evidence as to how they categorized the BES subsystems. If all/any BES subsystem elements that are not High or Medium are simply categorized as low, depending on what requirements CIP-003 - 009 bring forward, there could be undue and unjustified entity/consumer costs associated with implementation on BES elements that really do not require such.
Alliant	Agree	
Ameren	Disagree	Not all BES Cyber Systems for a High Impact BES Subsystems that perform functions for the BES should be considered critical. The cyber systems themselves should be evaluated for impact, see our comments on question 6. Yet, this draft standard proposes to categorize all these BES Cyber Systems as critical due to the categorization of the BES Subsystem.
Black Hills	Disagree	Until it is understood how CIP-003 through CIP-009 will be scaled for H - M - L criticality compliance, it is not possible to know whether CIP-002-4 will meet the objective. The concept is good, but not yet clear.
TNMP	Disagree	CIP-002-4 does not accomplish the objective because of problems with the current definitions used by CIP-002-4. The current draft is a good first attempt at meeting FERC's concerns; however, definition revisions and other clarifications requested by those submitting comments are needed to help paint the "bright lines" the drafting team is setting out accomplish.
NVEnergy	Disagree	Given the comments in the prior section, there is still some enhancement necessary to adequately accomplish the stated objective. We believe that the categorization as proposed in Attachment 1 to the proposed Standard may inappropriately assign High and Medium impact to various assets/subsystems that are not believed to have such a high degree of impact to the reliable operation of the BES. For example, the continued inclusion of blackstart generation systems as High Impact is in our opinion an overstatement of importance (particularly given that to classify it as such, it would demand the highest level of security protection, when in fact the importance of the blackstart systems is inconsequential except for the extremely rare instance that the systems are in use in a restoration event). We do concur that the basis and concept are correct: the application of security controls should be commensurate with the degree of impact that the subsystems

Organization	Yes or No	Question 2 Comment (Response page 14)
		have upon the reliable operation of the BES.
MWDSC	Disagree	Uncertain what, if any, security controls will be applied to a Low BES Impact. Without drafts of CIP-003 through CIP-009, how can CIP-002 be assessed for "applying security control commensurate with the potential impact"?
Empire	Disagree	I do not agree that the categories of Hi, Med, and Low, correctly identify BES Cyber Systems that support the functions critical to the reliable operation of the BES. There should also be a "No" impact category on those items that have no impact on the BES.
NCEMCS	Disagree	I have taken some extracts from existing comments and restated them in full support: The sole purpose of CIP-002 is to identify and categorize cyber systems according to their impact on the BES so we can apply appropriate security requirements to them. The listing of the Cyber System should be based on a top down approach rather than a bottom up approach. Only after a BES Subsystem is classified as a High or Medium Impact, should the Cyber System related to it should be classified as High, Medium Impact. Current CIP standards require an indirect assessment; a simple inheritance of impact from the BES Subsystem to its associated cyber systems without regard for the cyber system's actual function. We think this will result in the over-classification of many cyber systems. Having a purely BES Cyber System focused approach creates the issue of creating an inventory of hundreds of thousands of cyber systems and then performing an impact assessment of each one. This is wasteful of resources and will cause a great deal of work on the industry's part in large part focused on the lowest impact systems. All low impact BES assets have all associated cyber systems classified as low impact. This removes vast amounts of classification work. Since low impact is defined as having NO ability to directly impact the BES in any way, we would propose there be no requirements on this category. There is a danger of unintended consequences where the focus could shift from securing the high and medium impact systems to managing compliance on the several orders of magnitude more numerous ‘no impact’ systems. In the earlier versions it was a straightforward approach where the Registered Entity identified its Critical Assets (i.e., those assets that could affect the BES) and then you identified the supporting Cyber Assets and then the Critical Cyber Assets. My concern is for example: currently, if an entity determined through their RBAM that they have "no critical assets", then none of the controls and requirements of CIP-003 through -009 apply. Under this new proposal, let's assume the same entity would declare all assets to be "low impact". What type and level of security controls then apply to these "low" impact assets? None? (As per the old system?) Without information on the level of controls associated with this categorizing scheme, it is difficult to fully evaluate this concept. The V4 standard currently has criteria for High and Medium impacts and lumps all other BES Subsystems into Low, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule its potential impact. If there is even one requirement in the low impact category and that category is auditable and enforceable, the compliance evidence burden placed on entities will be onerous. Since there is no bottom to this standard and low is the ‘everything else’ category, every cyber system in the BES of North America will be on the list and in scope. There may be tens of thousands of systems per entity (would not each relay be a ‘cyber system’?). The majority of your compliance tracking and evidence gathering will be on the lowest impact, but orders of magnitude more numerous cyber systems. If the TFE process also applies to these millions of systems

Organization	Yes or No	Question 2 Comment (Response page 14)
		continent-wide we are creating an unmanageable bureaucracy. The standard needs minimum criteria. This has been stated many times I just want to re-enforce it "Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009, or a category for minimal-risk or no-risk subsystems must be created!" Since the Low impact category is simply a catchall, we propose there be no requirements for low.
SWTC	Disagree	Until the BES Definition is resolved, how can an entity identify and categorize BES Cyber Systems.
SCEG	Agree	
Exelon	Agree	
BPA Trans	Disagree	No, we do not agree that CIP-002-4 accomplishes the objective stated in the Purpose statement. The identification and categorization of BES Cyber Systems "commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES" is not achieved. R3.2 requires the Responsible Entity to "assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem." In most cases, this is appropriate as the most important consideration is the reliability of the BES. However, this may lead the over categorization of a BES Cyber System as it is "assigned" the same BES impact, rather than considering whether the effect of the BES Cyber System is significant or not. For example, a BES Cyber System might have Medium or Low BES Impact even though it is associated with a High Impact BES Subsystem.
HQT	Agree	
Allegheny Energy	Disagree	The approach utilized makes an effort to categorize BES assets but does not allow an opportunity to separately categorize BES Cyber Assets. The BES Cyber Asset inherits the impact categorization of the BES asset and creates a one-size fits all solution that may not be commensurate with their potential impact on the BES.
KCPL	Disagree	The goal is a lofty and extremely difficult one to hit. This effort, although noble, does not reflect the level of thoughtfulness required to establish the facility criteria necessary to draw a practical line in the sand to determine reliability impact at a High, medium or low level. In addition, there needs to be a "No Impact" level. It is not reality to assume that every element or combination of elements has a significant reliability impact.
Connectiv Energy	Agree	The Standard will allow the categorization of BES Cyber Systems, however this alone provides no guidance for what appropriate security controls are. Assuming that CIP-003 through CIP-009 are revised to recognize the categorization then the set will accomplish the larger purpose.
MidAmerican	Disagree	MidAmerican recognizes and understands the intentional shift in purpose from identifying Critical Cyber Asset Identification in CIP-002-2 to BES Cyber System Categorization in CIP-002-4. However, differentiating between high, medium and low may have little value or credibility for many security controls.

Organization	Yes or No	Question 2 Comment (Response page 14)
		When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. Further, security controls must be applied to distinct, discreet, individual Cyber Assets, not generically defined "systems." MidAmerican submits there is value in retaining the original purpose from CIP-002-2. MidAmerican's four proposed changes to CIP-002-2 are presented in question 13.
CPG	Disagree	This proposal does not take into account the criticality of a cyber system to the BES element, nor does it properly take into account the criticality of the BES element to the BES. What is lost in the proposal is that some cyber systems may not be critical to the operation or protection of the BES element, and would therefore not be critical to the BES. To have entities list every cyber system does not have an impact on the safety and reliability of the BES. The generator nameplate criteria, as well as control center MW criteria listed in Attachment 1 seem arbitrary. A discussion as to how those values were developed would be appreciated.
Santee Cooper	Agree	Once the impact levels are fixed, SC does believe it accomplishes the overall goal of protective requirements relative to their impact on the BES.
OGE	Disagree	• The intent is clearly there, however it is difficult to know how to assess the impact the BES due to the terminology. It is too subjective. • This revision, while a reasonable start at carrying out FERC's direction, does not provide enough meaningful detail so as to make the revised standard something the industry can confidently implement. For example, who decides whether or not something has "directly affected" the BES? What change in voltage for what length of time constitutes an "affect"? What is the difference between "directly affect" and indirectly affect? More definition needs to be provided on these kinds of terms.
Oncor	Disagree	It would appear to provide some additional flexibility, although the specific security controls are not yet defined.
PPL Supply	Disagree	Generally agree with EEI Comments. Devices which use a routable protocol that is remotely accessible pose a higher risk than those using a non-routable protocol or are on an isolated routable protocol network.
St. George	Agree	
NGRID	Agree	
MGE	Disagree	Do not agree with the Purpose statement since it does not give the applicable entities the clear and concise requirement(s) in order to fulfill the purpose statement. Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. The loss of a communication link to a BES Cyber System will not automatically cause

Organization	Yes or No	Question 2 Comment (Response page 14)
		the inability of equipment and/or electric system's thermo, voltage and stability limits that will cause instability, uncontrolled separation, or cascading failures. Recommend the purpose to read: To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) which could cause instability, separation or cascading to the Bulk Electric System (BES) as a basis for applying security controls.
FE	Agree	Per our prior comments, FE believes the purpose of this standard should be restated as "To identify cyber vulnerabilities that when breached could lead to BES instability, BES separation and/or a cascading sequence of failures." If the team retains its current path, the team should keep in mind that Low BES Impact as defined by this standard indicates a number of things that would NOT occur. The purpose statement is appropriately focused on functions "critical" to the reliable operation of the BES. Therefore, Low BES Impact Subsystems should require minimal or no security controls.
TECO	Disagree	We agree that the draft standard itself would accomplish this if the definitions were clarified, or removed in place of the attachment categorization. The phrase "BES as a whole" should replace BES at the end of the purpose. We also have great concern that the automatic inheritance of impact level of the cyber systems from Attachment 2 to the BES subsystems from Attachment 1 is problematic. This introduces many new cyber systems that do not have direct impact to the reliable operation of the BES subsystems, and is a significant departure from the approach that had previously been communicated by the drafting team. We believe that many cyber systems that currently reside on corporate networks will be pulled into scope. These include systems that do not directly impact BES reliability, that entities may have removed from their control system networks to achieve compliance with the existing set of standards. We foresee the need to create additional electronic security perimeters within corporate networks to accommodate the standards. The goal of these standards should be to protect those cyber systems that are critical to the reliable operation of the BES, not every cyber system associated with the BES.
CECD	Disagree	The purpose should include reference to the effort to categorize BES Subsystems as this is a significant task in this standard.
MRO	Agree	N/A
GTC	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not

Organization	Yes or No	Question 2 Comment (Response page 14)
		consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Xcel	Agree	
BGE	Disagree	We do not agree. It is too broad and has the potential to capture and bring in to scope items that are not critical to the reliable operation of the BES. The standard is diluted by not focusing on items that are that truly important to the security and reliable operation of the BES. We think that BES Cyber Systems without external computer and communications connections should be excluded. Next day planning systems should not be in scope. We believe that the proposed standard could result in secure BES Cyber Systems, without equivalent physical security protection. For example, it's possible to spend tremendous resources to secure BES Cyber Systems, and leave physical security gaps that would compromise the system.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although the drafting team has put in a lot of hard work and has tried to help identify and categorize those cyber systems, there's still some ambiguity. As mentioned in the subparts of question 1, we would like further clarification.
TAPS	Disagree	Because the proposed "low impact" category, as currently defined, would sweep in cyber systems that have no potential impact on the reliability of the BES, the standard would, as written, impose significant costs on responsible entities and Regional Entities with no commensurate benefit to reliability. See TAPS response to Question 1.i.
Allegheny power	Disagree	AP believes that it is important and appropriate to apply "security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations.
FMPA	Disagree	It does come close to doing so, FMPA has some comments on the details of how it is done, including the criteria of Attachment 1. The addition of new terms of "subsystem" and "functions" add complexity and ambiguity. How are these new functions related to the Functional Model, for instance? The real focus ought to be on the worst case contingencies / scenarios that can be caused by malicious manipulation of a cyber system. Such a focus bypasses the need to create new terms such

Organization	Yes or No	Question 2 Comment (Response page 14)
		as subsystems and functions. As such, the purpose ought to eliminate reference to the word "functions" and state: "To identify and categorize the BES Cyber Systems that support the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES."
Duke	Disagree	We believe that the proposed CIP-002-4 is too prescriptive, and that a better approach would be to use the "Cyber First" approach. See all of our other comments on CIP-002-4 for explanation and suggestions for improvement.
NBSO	Agree	
AESI	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
IESO	Disagree	Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we've got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): b. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. c. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined according to studies or other criteria determined by the RC. d. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring compliance.
Manitoba 2	Disagree	The current wording of the purpose and direction of the standard to include all BES Cyber Systems in the categorization will mean that security controls will be specified for BES Cyber Systems with a categorization of low. Any such identified security controls will then also be auditable. All BES Cyber Systems are not critical to support a BES Subsystem, and as such should not require auditable security controls. Guidance provided to industry on security controls for low impact

Organization	Yes or No	Question 2 Comment (Response page 14)
		BES Cyber Systems would be sufficient for the necessary strategic direction and would not require external audit of these low impact security controls. Inclusion of low impact BES Cyber Subsystem as auditable assets in the standard will significantly increase the implementation timeframe, increase the cost and will divert resources required to implement the controls associated higher impact levels. Auditable security controls in CIP-003 through CIP-009 should only be applied to high impact and medium impact BES Cyber Systems.
OMPA	Disagree	The draft standard assumes all cyber systems associated with BES assets have a definite impact on the reliability of the BES. We argue that treating every cyber system associated with a BES asset as a potential impact to the reliable operation of the BES could require extensive controls implementation that would have no net improvement on the reliability of the BES. OMPA urges the drafting team to consider a “no impact” option. OMPA also urges the drafting team to provide drafts of CIP-003-4 through CIP-009-4 for a better understanding of required controls prior to finalizing CIP-002-4.
ATC	Disagree	Suggestion: “To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) that affect the reliable operation of the Bulk Electric System.” Our proposed suggestion is attempting to clarify that the purpose of this standard is to only categorize BES Facilities.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 2 Comment (Response page 14)</th></tr>
<tr><td></td><td></td><td>instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>PSE agrees that the drafting team is headed in the right direction and fully supports their efforts. PSE also feels that not all the BES Cyber Systems have same reliability impact on BES systems. It would be helpful if the drafting team could bring some clarity in this standard to accomplish this objective with no room for interpretation. A BES Cyber System can have no impact for which CIP-002-4 does not seem to allow for especially if there is no remote access to it.</td></tr>
<tr><td>IMPA</td><td></td><td>IMPA has no comments</td></tr>
<tr><td>ERCOT</td><td>Disagree</td><td>ERCOT ISO recommends that the purpose be revised to address the identification and categorization of BES Subsystems as well as the BES Cyber Systems.</td></tr>
</table>

Organization	Yes or No	Question 2 Comment (Response page 14)
PacifiCorp	Disagree	PacifiCorp recognizes and understands the intentional shift in purpose from identifying Critical Cyber Asset Identification in CIP-002-2 to BES Cyber System Categorization in CIP-002-4. However, differentiating between high, medium and low may have little value or credibility for many security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just BES one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. Further, security controls must be applied to distinct, discreet, individual Cyber Assets, not generically defined "systems." PacifiCorp submits there is value in retaining the original purpose from CIP-002-2. PacifiCorp's four proposed changes to CIP-002.2 are presented in question 13.
IRC	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.
PEPCO	Disagree	We are very appreciative of the efforts of the SDT. In particular, we believe that it is important and appropriate to apply - security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES. This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations. And devices that have no remote access would have no impact on the BES system. With the draft standard, cyber assets inherit the same category as the BES asset, regardless of communications methods to control the CCA. Assigning BES cyber systems the same impact of the BES Subsystems does not seem appropriate. As was previously mentioned, high, medium or low categorization often has more to do with the connectivity of the asset (e.g. TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (e.g. if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For BES assets with no remote access, these should be classified as No Impact. If a cyber control system first approach is use, we would offer that the high, medium, or low would not be needed. Appropriate security measures/requirements would be based on the operating platform of the in-scope BES cyber control systems, the connectivity of the asset, and/or the span of control of the cyber asset's impact. At the same time, we would offer that not all cyber systems need to be considered and would be burdensome to do so. The challenge would be to limit the cyber systems to BES control systems and to identify the in-scope systems (e.g. SCADA, DCS, Microprocessor

Organization	Yes or No	Question 2 Comment (Response page 14)
		relays).
NEI	Disagree	A) The purpose as stated is flawed in that it does not deal with cyber vulnerability, which is the whole point of CIPs 002 through 009. NEI believes the purpose of this standard should be restated as "To identify cyber vulnerabilities that when exploited could lead to BES instability, BES separation and/or a cascading sequence of failures." B) If the team retains its current path, the team should keep in mind that Low BES Impact as defined by this standard indicates a number of things that would NOT occur. The purpose statement is appropriately focused on functions "critical" to the reliable operation of the BES. Therefore, Low BES Impact Subsystems should require minimal or no security controls. C) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Summary Consideration:

Organization	Yes or No	Question 3 Comment (Response page 15)
Progress Energy	Prefer method proposed in the standard	A proper judgment cannot be made on the proposed methods without knowing the ultimate impact of the other Version 4 CIP-003 through -009 standards. Both methods would ultimately require a full inventory of all BES assets and this process will not improve the overall reliability of the BES. If the proposed changes to the definition of Cyber System are made ("A discrete set of one or more routable or dial-up programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data."), then we are in agreement with the method proposed in the Version 4 standard.
Dynegy	Prefer method proposed in the standard	
GSOC/OPC		We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Hayden	Prefer alternative method	A decision tree / flow chart approach would be more effective and probably would provide more consistent results between Registered Entities.
SDGE	Prefer alternative method	
APPA	Prefer alternative method	APPA Task Force Comments: We believe each utility will need to inventory all BES connected Cyber Systems and then determine their level of impact on the BES based on the criteria in Attachment 1. See comments submitted in response to Question #6 below.
Consumers		Although we prefer the method proposed in the standard, substantial changes must be made in the process to gain our full support of the method. The suggested alternative method simply results in far too much analysis and documentation and appears as if it would result in the same list of assets that needs to be protected, yet through a much more onerous

Organization	Yes or No	Question 3 Comment (Response page 15)
		path. As noted earlier though, the current proposed method must be changed to allow for the separate (from the subsystem categorizing) secondary categorizing of the cyber assets. Neither method is recommended. The existing CIP-002-3 accomplishes what is needed. Taking a new course will lead to confusion and not result in any improvement in what has been accomplished to-date. If the concern is protecting the reliable operation of the BES, why is it not sufficient to have two categories of assets as in CIP-002 versions 1 through 3? Either something is critical or it's not... No matter how we choose to categorize and wordsmith, at the end of the day the same components will affect the reliable operation of the BES. Changing CIP-002 at this stage of the game is not going to reduce administrative overhead.
NPCC	Prefer method proposed in the standard	
MPPA	Prefer method proposed in the standard	
Central Lincoln	Prefer method proposed in the standard	You must categorize the electrical facilities prior to categorizing the associated cyber equipment.
Dominion	Prefer method proposed in the standard	Dominion recommends that BES assets be evaluated first and then the cyber systems (functions) be evaluated based on the criticality of the associated asset.
Encari	Prefer method proposed in the standard	The proposed method provides for specific scope limitations that are necessary during the discovery process, the alternate method would lead to an unnecessary inventory or nearly unlimited scope during the process. We are concerned about the transition process between the current CIP standards and version 4 as the identification of any additional Cyber Assets at this time only allow for one level of criticality whereas the new standard defines 3 levels. If version 4 of CIP-002 is to be adopted without updating the remaining CIP standards simultaneously it will lead to confusion as to which requirements pertain to which Cyber Assets. We recommend developing a mapping of the current mandatory requirements to the 3 categories. The proposed method also is missing specific elements within attachment 2. For instance, we have identified situations where BES Cyber Systems included for reducing emissions may impact a BES Subsystem indirectly. We also recommend further addressing security controls for remote vendor support as it is incredibly important for day to day operations and emergency conditions. Although indirect components can lead down a very difficult path to properly inventory and limit, these cases should be reviewed for inclusion.

Organization	Yes or No	Question 3 Comment (Response page 15)
US ACE – NW	Prefer method proposed in the standard	
SCE	Prefer alternative method	Since the genesis of the NERC CIP standards was the protection of BES assets by providing security to the cyber assets supporting BES functions, SCE believes that risk analysis should be driven by the function of the respective BES assets. A cyber asset first approach should be used to identify connectivity types and cyber asset functionality based on Attachment 2. The level of security controls can then be determined based on BES criticality as identified in Attachment 1.
USBR	Prefer alternative method	This question is poorly worded in that you cannot disagree with Attachments 1 or 2, which happens to be the case. As indicated in previous answers the alternative method is create a criteria for assessing impacts of elements. This proposed process can easily result in over categorization of elements which will not result in increased reliability. The focus needs to be on those functions which can harm the reliability of the BES (have an impact. This standard touches on some of the issues which need to be addressed in the assessment criteria. It is unrealistic to assess 20 MW units against a 2000 MW requirement. However, the responsible entity (lets say GO) should communicate with its TO, BA or RC, to determine if the TO, BA, or RC relies on the facility for specific reliability functions (AGC or AVC). In some WECC balancing authorities a 200 MW Pump Storage plant may be relied heavily for AGC. On other WECC balancing authorities 200MW is decimal dust.
Dyonyx	Prefer method proposed in the standard	While we prefer the proposed method in the standard, we believe there is some risk that independent “Elements” that are not directly related to a specific BES Cyber System may be missed if a complete inventory is not conducted.
MISO	Prefer method proposed in the standard	
Westar	Prefer method proposed in the standard	
Green Country		Neither to do a proper assessment you would have to work it both ways to make sure all were included. Again no "Bright Lines" are drawn. Also to preclude an interpretation. Do you have to only have 1 sub element in for example Dynamic Response to have a Dynamic Response function? i.e. Power system stabilizers and nothing else. OR Must you have all of the sub elements listed for each respective function?
Oregon PUC		No comment

Organization	Yes or No	Question 3 Comment (Response page 15)
NB Power Gen	Prefer method proposed in the standard	
Manitoba 1	Prefer method proposed in the standard	Need more time to review
Portland GEG	Prefer method proposed in the standard	PGE does not have a preference, however, we are marking that we prefer the method in the standard because it is most similar to current methodology.
PSEG	Prefer method proposed in the standard	Comment #1: After reviewing both approaches, they seem to result in the same list of BES Cyber Systems. Comment #2: The existing CIP-002-3 accomplishes what is needed. Taking a new course will lead to confusion and not result in any improvement in what has been accomplished to-date. Comment #3: 1. Criterion 1.3. would assign a “High BES Impact” to generators that have been “pre-designated” as Reliability Must Run units. Whether a generator is High Impact, Medium Impact, Low Impact or No Impact has nothing to do with the label an RTO/ISO slapped on it to keep it from being retired. The assignment of “High BES Impact” should be based on a sound engineering evaluation, not on a label. 2. Criterion 1.11. refers to “frequency related instability.” There is no such thing as “frequency related instability” for transmission. The accepted categories of transmission stability are as follows: (1) steady-state stability; (2) transient stability; (3) small signal stability; (4) voltage stability. This error can be fixed by simply deleting the words “due to frequency related instability.” 3. With the recommended fix to Criterion 1.11. (see (3) above) Criterion 1.10. can be deleted. 4. Attachment 1 uses a number of euphemisms to refer to undesirable outcomes, e.g. “electric system collapse,” “complete operational failure of the transmission system” and “separation.” The authors of Attachment 1 need to stick to terminology found in the lexicon of power system engineers and clearly communicate just what the standard is. The indiscriminate use of vague terminology in standards will lard up the cost structure of competitive generators with no possibility of recovery. 5. Criterion 1.7. is way off the mark. The fact that a contingency requires implementation of a TLR says nothing about whether the facility is High Impact, Medium Impact, Low Impact or No Impact. TLRs are routinely implemented in operational circumstances that have no impact at all. This Criterion needs a lot of work; as written it arbitrarily assigns “High Impact” status to events that are routinely encountered in the day-to-day operations. Overall, Attachment 1 needs addition rework. Generators must be sensitive to the needs of the competitive business they are in and not be subjected to cost increases that add little enhancement to overall reliability. Vagueness and ambiguity

Organization	Yes or No	Question 3 Comment (Response page 15)
		will undermine the competitive business generators are in. With proper attention to precise engineering terminology and performance instead of generalities, the number of criteria in Attachment 1 can be greatly reduced.
WE-Energies	Prefer alternative method	Wisconsin Electric Power Company supports EEI's comments regarding this question. In addition, we support an alternative approach as put forth by several entities. This includes the use of a "cyber first" approach to asset classification and impact to the BES. This would include: • Identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment 2. • Identification of control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate as "high impact" cyber assets to the BES • "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use would be classified as "medium impact" cyber assets.
Idaho Power	Prefer alternative method	The criteria in Attachment 1 is more applicable to categorization of BES subsystems than BES Cyber systems. Another alternative would be to inventory BES cyber systems and categorize by their impact on the critical functions.
SOCO	Prefer alternative method	In the matter between the BES Subsystem focus vs. the BES Cyber System focus, Southern Company supports a hybrid approach. The sole purpose of CIP-002 is to identify and categorize cyber systems according to their impact on the BES so we can apply appropriate security requirements to them. In order to accomplish this, we need to know the impact of the cyber system, not solely the impact of BES Subsystems. Current CIP standards require an indirect assessment; a simple inheritance of impact from the BES Subsystem to its associated cyber systems without regard for the cyber system's actual function. We think this will result in the over-classification of many cyber systems. For example, a high impact substation may contain a fault recorder whose function is to collect data for future analysis and a relay on a 500kV line to a peer utility. The impact to the BES of those two cyber systems are vastly different and both do not need to be declared high impact and meet all the same requirements due solely to the substation's impact level. However, having a purely BES Cyber System focused approach creates the issue of creating an inventory of hundreds of thousands of cyber systems and then performing an impact assessment of each one. This is wasteful of resources and will cause a great deal of work on the industry's part in large part focused on the lowest impact systems. We propose a hybrid approach: 1. The Planning Authority performs an engineering analysis utilizing 'bright line', well-defined parameters that are consistent across the interconnection. The result of the engineering analysis is a list of BES assets classified according to impact. Bright line parameters would also have to be determined for control centers based on the aggregate of controlled assets.

Organization	Yes or No	Question 3 Comment (Response page 15)
		2. All low impact BES assets have all associated cyber systems classified as low impact. This removes vast amounts of classification work. Since low impact is defined as having NO ability to directly impact the BES in any way, we would propose there be no requirements on this category. There is a danger of unintended consequences where the focus could shift from securing the high and medium impact systems to managing compliance on the several orders of magnitude more numerous 'no impact' systems. 3. For the medium and high impact BES assets, we switch to the cyber system focused approach. The associated cyber systems are inventoried and each is classified as to its direct impact based on their "span of control"; how many MW's of load or generation are at risk from this cyber system should it be compromised, misused, or degraded. In conclusion, we use the BES Subsystem/Engineering Analysis approach as a first filter to quickly handle the quantities of low impact cyber systems, then we switch to the BES Cyber System focus to get a truer impact determination for the medium and high impact cyber systems. The control system for a Generation Unit may be classified as a High Impact, but classification of a condenser air in-leakage monitor, which is neither remotely accessible nor essential for generation should not required to be classification at the component level.
DTE	Prefer method proposed in the standard	Either method should produce the same list.
AEP	Prefer alternative method	Refer to question #2 above.
Edison Mission	Prefer method proposed in the standard	While we prefer the proposed method in the standard, we believe there is some risk that independent "Elements" that are not directly related to a specific BES Cyber System may be missed if a complete inventory is not conducted.
Calpine	Prefer method proposed in the standard	
NS&T	Prefer alternative method	We believe it is appropriate to consider impact(s) on BES, but we believe impact criteria should be simplified.
E ON	Prefer alternative method	Attachment 1 provides a list of facilities to be classified as High and Medium impact BES Subsystems. That is all that should be needed. Attachment 2 includes functions, such as providing reserves and facilities used in shedding load that would render nearly every generating unit or distribution feeder critical to BES reliability. That is not the case and the

Organization	Yes or No	Question 3 Comment (Response page 15)
		costs of proceeding in this manner promise to far outweigh the incremental enhancement to BES reliability, if any. E ON U.S. notes that CIP-002 Attachment 1 section 1.2 is unclear as to whether the reserve obligation is that of the reserve sharing group or the participating member. It should be of the group as a whole otherwise the economic and operational benefits of reserve sharing could evaporate. This would of course depend on the requirements of the as yet unseen CIP-003-009 V4 standards. Section 1.7, 1.8, 1.10, 1.11, 1.12 should be limited to an appropriate planning scenario. There is no end to the operating scenarios one might conceive that would result in the sorts of adverse reliability outcomes these sections each describe. At some point risk has to be defined in a rational and objectively measurable manner. Section 1.6 should be limited to an identified primary Cranking Path as opposed to all conceivable Cranking Paths.
Carthage	Prefer method proposed in the standard	CWEP feels that Attachment 2 should be eliminated because it causes confusion. CWEP feels that the functions listed in Attachment 2 should be specifically covered in Attachment 1 under the impact categories they fit. The way the attachments are designed leaves too much room for interpretation. CWEP is okay with the format of the standard but would like for the criteria to be more specific.
WECC	Prefer alternative method	The First method provides a simpler method of generating a list, and would be easier to audit to the standard. The alternative method provides for a more comprehensive evaluation and could potentially find assets that are critical to the BES that are not specifically classified in Attachment 1 or that are identified at a later time without needing to update the standard. If the alternative method were used, Requirement 3 would need to be updated to match.
Entergy	Prefer alternative method	The purpose of CIP-002-4 is to define the process Responsible Entities must use for identifying in specific terms the 'scope of applicability' of the rest of the CIP Standards for the grid infrastructure owned/operated by each Entity respectively. This process should approach the matter using a logical top-down methodology, beginning with identification of "Functions Essential to Reliability of the BES" as identified in Attachment II to the CIP-002-4 draft standard. From there, the method should proceed with identification of cyber assets used to implement said "Functions," followed by categorization of those cyber assets based upon potential adverse impact on reliable operation of the BES (as a functioning 'system') posed by the different types of cyber assets themselves. It's the potential impact of various cyber exploits or compromises presented by different types of cyber assets that dictate the need for a hierarchy of security controls and countermeasures, not categorization of BES equipment, sites, etc. based on type, size, facility rating, etc.
CenterPoint	Prefer method proposed in the standard	Although CenterPoint Energy believes the asset-based methodology in the existing version of CIP-002 is preferable to the subsystem-based methodology proposed in version 4, CenterPoint Energy believes the method proposed in version 4 is preferable to the alternative approach presented in this question.
LCRA	Prefer method proposed in the standard	

Organization	Yes or No	Question 3 Comment (Response page 15)
FRCC		As noted in a previous comment, I am not sure why you need the definitions of subsystems etc since you have specific criteria identified in both Attachments.
NIPSCO	Prefer method proposed in the standard	After reviewing both approaches, they seem to result in the same list of BES Cyber Systems. Suggestion: Clarify what the SDT views would be the impact of reversing the approach.
ConEd	Prefer method proposed in the standard	
EEI		EEI believes that while there may be some value in identifying and characterizing significant facilities such as large generating facilities, large transmission substations, or control centers, the real opportunity is to identify and characterize the cyber systems that are required to keep these facilities and functions operational.
O&R	Prefer method proposed in the standard	With consideration of comments in question 2.
Alliant	Prefer method proposed in the standard	We agree with the method in principle, however, see answers to questions 8 and 12 for specific comments on Attachment 1 and 2 criteria.
Ameren	Prefer method proposed in the standard	Responsible Entities should be allowed the choice of either method. Until a thorough analysis is performed by each entity, they should be allowed the option to define their methodology either way. If we had to choose today without time to evaluate each option we would select the proposed method. In either case Attachment 1 and Attachment 2 need to be modified as suggested in our comments in questions 8 and 13.
Black Hills	Prefer method proposed in the standard	Regardless of the order processed, both categorizations must be completed. The process will likely be iterative, so the order doesn't matter. The approach described in CIP-002-4 most closely matches the work done by entities already, which is the basis for BHC's preference.
TNMP	Prefer method proposed in the standard	TNMP finds the proposed standard method more manageable than the alternative of inventorying all BES Cyber Systems. Keeping track of BES Cyber Systems for BES Subsystems that are of Low BES Impact would take away the limited manpower to focus on maintaining massive documentation for an audit and exposes Entities to findings that are not significantly relevant to the security of the BES. If a Responsible Entity had far more Low than High or Med BES Impact Subsystem then much time would be spent maintaining documentation for an audit. Why spend the time for a system that is recognized as having Low BES Impact and thus probably would not be subject to future CIP-003 through CIP-009 revisions? Let the Responsible Entity use its resources to focus on the BES Cyber System that are more likely

Organization	Yes or No	Question 3 Comment (Response page 15)
		to have a High/Med BES Impact.
NVEnergy	Prefer alternative method	The security controls prescribed by the subsequent CIP Standards must be targeted toward those cyber systems that are essential to the reliability of the BES and are associated with a function of the BES subsystem that has significant impact on the BES. Given that the engineering and planning of the BES is such that single contingency failures can be accommodated under the most extreme circumstances, categorization strategies for the CIP purposes that begin with the classification of the BES facilities is inappropriate. The revised CIP standards should focus first upon the cyber devices that can be compromised; then proceed to a determination of what degree of impact that compromise might have upon the BES.
MWDSC		Prefer none of the above. Recommend separating the transmission from generation criteria in the attachments and including more specific technical criteria such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Prefer alternative method	A preferred method would be: Step 1-Inventory all BES Cyber Systems Step 2 Identify all related BES Subsystems Step 3-Categorize based on Attachment 1 Step 4-Notify neighboring TO Step 5- Review and update lists
SWTC	Prefer alternative method	
SCEG	Prefer method proposed in the standard	
Exelon	Prefer alternative method	Exelon believes that the standard should first consider the cyber system vulnerabilities and then determine the potential impact to the reliability of the BES.
BPA Trans	Prefer method proposed in the standard	We marked “Prefer method proposed in the standard” as it most closely matches the current Critical Asset and Critical Cyber Asset methodology. It appears that definitions described in the rest of the document allows BES Cyber Systems to be classified as BES Subsystems. We do not believe that this is correct. Cyber Systems support the reliability functions of the BES Subsystems, not the other way around.

Organization	Yes or No	Question 3 Comment (Response page 15)
HQT	Prefer method proposed in the standard	
CCG	Prefer alternative method	Concerns remain about whether this approach effectively addresses reliability vulnerabilities without unnecessarily requiring controls on assets that do not impact reliability. We support further development and consideration of an approach that starts with an analysis of cyber assets.
Allegheny Energy	Prefer method proposed in the standard	
KCPL	Prefer alternative method	Attachments 1 and 2 are good lists of all the reasons to determine and provide protections for the cyber infrastructure underlying the monitoring and control of the BES. However, neither of these attachments in any combination are sufficient to provide the level of guidance necessary to draw appropriate conclusions. The way this is proposed could involve every generator, transmission line, bus, breaker and transformer. Apparently, it is not sufficient for Registered Entities to develop a process for the determination of reliability impact of their facilities and this proposal does not sufficiently establish the criteria to make that same determination. Although I do not disagree with the concepts being promoted here, namely a process to classify facilities and equipment such as HIGH, MEDIUM, and LOW, the criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to "plug into" this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
Connectiv Energy	Prefer method proposed in the standard	
MidAmerican	Prefer alternative method	1. Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. 2. Change CIP-002-2 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in CIP-002-2. 3. Change CIP-002-2 R3 to use "the list of BES assets" instead of "the list of Critical Assets." Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility.

Organization	Yes or No	Question 3 Comment (Response page 15)
		4. CIP-002-4 must be implemented on the same schedule as revised security controls. 5. Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunities to move forward with CIP-002 and to prove what categorizations will be meaningful. The existing work from the proposed approach would then be validated or revised based on its applicability to the security controls.
CPG	Prefer alternative method	The prior version of CIP-002 considered two dimensions of risk. The first dimension of risk considered was impact, which was whether or not a cyber asset was associated with a critical asset. Secondly, it considered vulnerability by determining whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal, the SDT has eliminated any consideration of the risk due to vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest categories of varying degrees of vulnerability (high and low) be added to the criteria in Attachment 2. Furthermore, understanding the design basis threat against which mitigation measures may be built is fundamental in creating an effective set of control measures. The threat potential basis should be clearly established. In addition, time and effort should be given to development and consideration of a “cyber first” approach. We appreciate that the proposed version seeks to protect the assets most critical to the bulk electric systems. However, the direction of this proposal may be missing some vulnerabilities and drawing some assets into scope that have little if any impact on reliability. For any approach taken, it is important to remain focused on reliability.
Santee Cooper	Prefer alternative method	Also noting that both Attachments need re-work.
OGE	Prefer alternative method	I would prefer a hybrid where you categorize the BES Subsystems and then assess the risk of the cyber assets and the potential impact on the BES Subsystem.
Oncor	Prefer alternative method	More intuitive approach.
PPL Supply	Prefer alternative method	Agree with EEI comment.

Organization	Yes or No	Question 3 Comment (Response page 15)
St. George	Prefer alternative method	We are also very concerned about the timetable of CIP-002-4 in relation to the accompanying standards CIP-003 through CIP-009. Entities should be able to know the requirements imposed on certain classifications before commenting on criteria that place entities in said classifications. CIP-002-4 comments should be open during the same period as CIP-003-4 through CIP-009-4.
NGRID	Prefer alternative method	The reference framework of electric grid engineering, facilities ratings, etc listed in Attachment 1 is not required and the alternative method sans the Attachment 1 criteria will be a better approach since the issues at hand needs to be approached from a networked-computing systems security engineering perspective.
MGE	Prefer alternative method	A NERC Standard only needs to state “what” has to be accomplished not “how” the entity shall meet the requirements. This question is not in line with the actual requirements of 1 and 3. Both R1 and R3 start with “As a step in…”. Neither requirement states that R1 or R3 have to follow any order, the requirements do state that R1 and R3 are steps (processes) used to identify categorize an entity’s BES Cyber Systems. Please clarify this question.
FE		We do not prefer either alternative as indicated above. The use of the term "Subsystem" in Attachment 1 and the various Subsystem definitions that include direct linkage to a Cyber System ensures that Attachment 1 is not merely a "Big Iron" approach of categorizing electric grid assets ignoring Cyber Systems. Therefore, the existence of a Cyber System is a prerequisite to its Subsystem components that are being considered. In other words, a cyber review is not something that would occur subsequently. Rather than having Attachment 1 drive a High/Medium/Low categorization FE proposes that Attachment 1 appropriately provide the Subsystems that if compromised could lead to a High BES Impact (cascade, instability, etc.). Accordingly we propose a re-work of Attachment 2 such that it would direct appropriate High/Medium/Low categorization for controls and countermeasure requirements in CIP-003 through CIP-009 that reflect the differences in the Cyber System classification. In layman terms, routable technologies would be High, dial-up Medium and legacy serial communications would be Low. FE believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
TECO	Prefer alternative method	We support the “Cyber First” methodology as described in Entergy’s Comments. We believe that this will drive a matrix approach to include both the impact and risk of probability of exploitation associated with the cyber system. We believe that the impact level of the cyber system should be directly tied to the load controlled by that cyber system. We believe that routable protocols that could be used in sophisticated or coordinated attacks against a large portion of the grid should be considered higher risk of exploitation and serial or non-routable protocols that would be limited to targeted attacks on specific equipment should be afforded a lower risk. Entergy’s comments further explain this approach. If this methodology is adopted, we believe that much of the concern about specific Critical Assets related to generation would be resolved. We also believe that much of the current CIP002 V4 draft would change, which in turn would change

Organization	Yes or No	Question 3 Comment (Response page 15)
		our consideration of the other questions on this comment form.
CECD	Prefer method proposed in the standard	Subject to modifications as described, including the ability to identify assets that have no BES impact, CECD supports a process for evaluation of the BES assets impact on the system prior to engaging in listing BES Cyber Systems. CECD does not encourage a cyber first approach to the extent such an approach jeopardizes the BES threshold which is very important to prevent an overly broad application of these requirements, including impact to demand response programs at the consumer level.
MRO	Prefer method proposed in the standard	We agree with the method in principle, however, see answers to questions 8 and 12 for specific comments on Attachment 1 and 2 criteria.
GTC		We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Xcel	Prefer method proposed in the standard	
BGE	Prefer alternative method	We feel that a better sequence for identifying high impact BES subsystems would be to start with an analysis of cyber assets to first evaluate those systems that control or impact operations of the BES, rather than starting with generation or transmission assets, and determining which of those are high impact. To the extent that Attachment 1 remains a part of the standard, we offer the following revisions: (High Impact BES Subsystems): 1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or Low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability “must run” units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan. Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem. 1.5. Each Transmission Subsystem that contains switching stations substations operated at 300 kV or higher in the

Organization	Yes or No	Question 3 Comment (Response page 15)
		Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines leaving the station. 1.6. Each Transmission Subsystem comprising the Cranking Paths. 1.7. Each Transmission Subsystem that, if lost, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method consistent with FAC-10. 1.8. Each Transmission Subsystem that, if lost, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We feel that 1.9 was duplicative with the presence of 1.1-1.4 and 1.8 1.9. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above. The group felt that 1.10-1.12 were duplicative with the presence of 1.7 1.10. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse as determined through an engineering evaluation or other assessment method. 1.11. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. 1.12. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages. 1.13. Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more New proposed element: 1.17. Each BES Subsystem whose loss qualifies as a category C or D event according to TPL-001-1. * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and

Organization	Yes or No	Question 3 Comment (Response page 15)
		that functional entity submits a written request for the information. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.
Springfield, MO	Prefer alternative method	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Prefer method proposed in the standard	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Prefer method proposed in the standard	
FMPA		Neither. Both the concepts of Subsystems and functions are unnecessary and add confusion and complexity to the standard. The focus of the standard ought to be on the Cyber Systems themselves, and the criteria for which we define High, Medium and Low BES impacts to those Cyber Systems. Instead, we recommend identifying the worst case contingencies / scenarios that can be caused as a result of a Cyber System rendered unavailable, degraded or compromised, and compare the contingencies / scenarios with the criteria of Attachment 1. In this way, we assign High, Medium and Low impact directly to Cyber Systems without unnecessary middle steps of defining Subsystems and functions. This, of course, would require an inventory of Cyber Systems, but, such an inventory would already be necessary to enable the definition of Subsystems anyway, so, defining Subsystems is an unneeded step in the process.
Duke	Prefer alternative method	We believe that an alternative method is preferable. The first step should be to identify the BES Cyber Systems that can impact functions which are essential to BES reliability. By beginning with an examination of what the various interconnected Cyber Systems can affect, and then ranking them based upon their potential impacts, an entity can better determine the direct impacts, aggregated impacts due to interconnection, as well as common mode vulnerabilities.
NBSO	Prefer method proposed in the standard	
AESI	Prefer	We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its

Organization	Yes or No	Question 3 Comment (Response page 15)
	alternative method	benefits.
IESO	Prefer method proposed in the standard	
Manitoba 2	Prefer method proposed in the standard	The cyber-up approach creates a list of a large number of assets which would need to be auditable and managed for any changes.
OMPA	Prefer alternative method	For Requirement 1, OMPA suggests "…each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria …". Many entities are owners that do not operate the BES subsystems. Security controls should be based on operation, not ownership.
ATC	Prefer method proposed in the standard	
LES	Prefer method proposed in the standard	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 3 Comment (Response page 15)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Prefer method proposed in the standard</td><td>It is imperative that the standard effectively achieves the proper security controls and ensures reliability without being requiring resources to focus on documenting, evaluating, and categorizing what is not really important. It seems that the proposed method of categorizing high and medium BES Subsystems and then determining BES Cyber Systems based on critical functions identified in Attachment 2 and bounded by points of vulnerability associated with remote access would ensure entities focus on the important things.</td></tr>
<tr><td>IMPA</td><td>Prefer method proposed in the standard</td><td></td></tr>
<tr><td>ERCOT</td><td>Prefer method</td><td></td></tr>
</table>

Organization	Yes or No	Question 3 Comment (Response page 15)
	proposed in the standard	
PacifiCorp	Prefer alternative method	1. Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. 2. Change CIP-002-2 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in CIP-002-2. 3. Change CIP-002-2 R3 to use "the list of BES assets" instead of "the list of Critical Assets." Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility. 4. CIP-002-4 must be implemented on the same schedule as revised security controls. 5. Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunities to move forward with CIP-002 and to prove what categorizations will be meaningful. The existing work from the proposed approach would then be validated or revised based on its applicability to the security controls.
PEPCO	Prefer alternative method	Modified cyber approach: If a cyber control system first approach is use, we would offer that the high, medium, or low would not be needed. Appropriate security measures/requirements would be based on the operating platform of the in-scope BES cyber control systems, the connectivity of the asset, and/or the span of control of the cyber asset's impact. At the same time, we would offer that not all cyber systems need to be considered and would be burdensome to do so. Please reference discussion of Cyber System. We would propose a method that would identify the BES Cyber Control systems. These should be limited and the in-scope systems (e.g. SCADA, DCS, Microprocessor relays) should be identified. With the standards identifying appropriate security measures/requirements based on specific criteria (e.g. operating platform, connectivity of the asset, span of control of the cyber asset's impact) there would be no need to review the big iron other than for the span of control. We believe that this modified cyber first approach would mitigate the administrative burden of the existing cyber security standards and the proposed methods and get closer to the goal, the purpose of the standards, and moves us toward performance based requirements.
NEI	Prefer alternative method	A) This process should approach the matter using a logical top-down methodology, beginning with identification of "Functions Essential to Reliability of the BES" as identified in Attachment II to the CIP-002-4 draft standard. From there, the method should proceed with identification of cyber assets used to implement said "Functions," followed by categorization of those cyber assets based upon potential adverse impact on reliable operation of the BES (as a

Organization	Yes or No	Question 3 Comment (Response page 15)
		functioning 'system') posed by the different types of cyber assets themselves. It is the potential impact of various cyber exploits or compromises presented by different types of cyber assets that dictate the need for a hierarchy of security controls and countermeasures, not categorization of BES equipment, sites, etc. based on type, size, facility rating, etc. B) Alternative Top-down argument for defining the correct CIP Standards' Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue. • N-1 engineering also dictates that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on the perpetrator's ability to *navigate* across and between control system data networks to *access* multiple sites. C) Another Alternative: The existence of a Cyber System is a prerequisite to its Subsystem components that are being considered. In other words, a cyber review is not something that would occur subsequently. NEI proposes a re-work of Attachment 2 such that it would direct appropriate High/Medium/Low categorization for controls and countermeasure requirements in CIP-003 through CIP-009 that reflect the differences in the Cyber System classification. In layman terms, routable technologies would be High, dial-up Medium and legacy serial or other non-routable communications would be Low. NEI believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. D) Need to define screening criteria for when cyber applies. E) Need to clarify "the potential to adversly impact". F) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems.

1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."

Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Organization	Yes or No	Question 4 Comment (Response page 16)
Progress energy	Disagree	We cannot agree with the categorization without knowing the ultimate impact of the CIP-003 through -009 Version 4 standards. Change 1.1 from "…within 30 calendar days of the completion of the change" to "…on an annual basis".
Dynegy	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets."
GSOC/OPC	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing "within 30 calendar days of the completion of the change" with "within 30 calendar days of the Responsible Entity becoming aware that the change has occurred". Also, to clarify applicability, we suggest replacing the phrase "that could affect the impact of BES Subsystems" with "that could affect the degree of impact of the Responsible Entity's BES Subsystems." For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a

Organization	Yes or No	Question 4 Comment (Response page 16)
		timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
SDGE	Disagree	We are advising that the 30 day timeframe is too short for the work that needs to be completed. The 30 days typically includes the time required to do studies and then get approval from the Reliability Coordinator. We suggest the 30 day timeframe apply to providing the study results to the RC. While commissioning of new BES Subsystems is addressed, the acquisition of existing BES Subsystems is not addressed in R1.
APPA	Disagree	We disagree with the need for BES Subsystem identification as discussed below under Question #6.
Consumers	Disagree	Under the proposed regulation, in order to properly classify a generation subsystem, the generator owner and generator operator need to be provided information from the transmission operator and reliability coordinator. There are no requirements in the proposed standard for the transmission operator or reliability coordinator to provide such information. Without such requirements in the standard, the generator owner and generator operator should not be held liable for non-compliance due to failure of the transmission operator and reliability coordinator to provide the required information. The requirement in R1 should be modified because the goal is not to identify "appropriate security controls for its assets", but rather the same for its critical (high impact, essential, call it whatever) cyber assets or cyber systems. The requirement for producing a list has not yet been introduced within the document. A list is discussed in R3, but that is a list of cyber systems. On the surface, 30 days seem to be a reasonable time-frame to update the (yet undefined) list. However, we are concerned that some projects to place a subsystem in service (such as a small change or addition to and existing facility) may not give adequate time for all the ensuing requirements that come from CIP-003 >> CIP-009. In addition, there are REs that currently only have Control Centers (and associated Cyber Assets) and a few substations (with NO critical cyber assets) as critical, so these REs have not had to implement CIP-003 >> CIP-009 in a field environment. As one can imagine, doing so if a far greater challenge than the controlled environment of a control center and will be much more difficult. The 30 day period would not be nearly adequate time to implement cyber security controls in this instance. As such, we suggest the requirement be change to at least 60 days. The inclusion of "… or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System" is too vague as a trigger for having to update the list. Specific criteria needs to be introduced instead. We believed the annual review of the critical asset list and critical cyber asset list in the previous versions of the standard was appropriate and such a review should be required here as well.
NPCC	Disagree	RC should be removed from 1.2.
SWPA	Disagree	Updating the categorized list of BES subsystems within 30 calendar days of completion of any change to a BES

Organization	Yes or No	Question 4 Comment (Response page 16)
		subsystem is too short a time period for Responsible Entities to assess the impact of the change and update its list. Suggest lengthening the time period from 30 days to 90-120 days.
MPPA	Agree	MPPA concurs with the intent of the requirement, but that R1.2 needs to be clarified. 1) The engineering evaluation or other assessment method needs standardization so it is applied consistently throughout the industry. 2) Does the responsible Entity develop a methodology to be approved by the Reliability Coordinator or Reliability Assurer? Or, does the Reliability Coordinator or Reliability Assurer provide an approved methodology to be used by the Responsible Entity? As written, this requirement does not clarify who provides the assessment method.
Central Lincoln	Disagree	Central Lincoln fails to see why the yearly requirement of the present version presents an unacceptable risk to reliability. This will be a burden on those entities that are actively updating their systems, and will provide a disincentive to do so. This could harm rather than improve reliability. 1.2 is ambiguous. Must the "engineering evaluation" be approved by the Reliability Coordinator or Assurer, or just the "other" method(s)? From the webinar, it seems the SDT intended that both need approval, but this is not clear in the standard as written. There is presently no requirement for RCs or RAs to perform any assessment of an entity's evaluation. CIP-002 or another standard should include a requirement for RCs/RAs to perform these assessments when asked, and within a reasonable time period of such a request. As written, the standard expects registered entities to produce the approvals of other entities not under their control and under no obligation to help.
NERC	Agree	1. In order to support compliance activities, add the following and update the Measures section appropriately: R1: add text to require signed and dated (by proper personnel identified per CIP-003 / R2) reviews on a periodic basis (at least annually) of the categorization of BES Subsystems under the entity's ownership. R1.2: add text to require signed and dated (by proper personnel identified per CIP-003 / R2) documentation of all engineering evaluations or other assessment method(s) approved by the RC or RA(?). If an evaluation or assessment was required, include signed and dated (by proper personnel identified per CIP-003 / R2) documentation of the request to and response from the RC or RA(?). 2. The term Reliability Assurer is used in the standard but is not yet an official NERC Glossary Term. It needs to be added to the definitions being proposed. 3. Requirement R1.1 – the list of activities for which an update is required should specifically include when a Responsible Entity is notified of a change per Requirement R2. Similar updates are needed in the Measures section. 4. Requirement R1.1 – replace the word "impact" in line 4 with "categorization". 5. Requirement R1.2 – the expectation that study based assessment methods would be acceptable to classify or change impacts violates a core principle of the activity as stated in the supporting guidance document. Page 4

Organization	Yes or No	Question 4 Comment (Response page 16)
		Paragraph 2 states that the impact "thresholds are defined to provide a straightforward and objective path …to determine impact categorization…" The use of engineering evaluations or other assessments results in a much less objective and potentially inconsistent application of the categorization process, requires a significantly higher level of resource commitment to perform the evaluations, and introduces the need for Reliability Coordination or Reliability Assurer oversight/validation. Further, for some of the impact criteria such as frequency response, sufficient quality models do not exist upon which evaluations could be reliably based to determine system collapse. This significantly undermines the "bright-line" approach intended and therefore is counter to the team's stated goals in this effort. These study-based methods need to be minimized or eliminated and the bright-lines more clearly defined.
Dominion	Disagree	To satisfy CIP-002-4 R1.1, entities will need to know what changes could affect the impact of BES Subsystems on the Bulk Electric System. It can be inferred from this premise that Responsible Entities who possess the capability to determine those changes would have an obligation to identify such changes. The entities with such capability typically consist of one or more of the following: Reliability Coordinator, Balancing Authority, Transmission Operator and/or Regional Entity. Dominion suggests that a requirement be added to ensure that such entities develop appropriate criteria to identify such changes. While Dominion agrees with most portions of requirement R1.2, some modifications are needed. Specifically, Dominion suggests that: 1) Reliability Assurer should either be added to Applicability Section 4.1 or it should be removed from R1.2; and 2) a specific requirement should be added for each Reliability Coordinator or Reliability Assurer to identify their approved engineering evaluation or other assessment method(s).
Encari	Disagree	We agree in theory with this requirement; however, we express concern over the implementation timetable for any modification of the BES subsystems within an entity. We have encountered many situations that due to system failures associated with Critical Assets that new critical assets are identified. It is very important to handle these BES Subsystem situations associated with unplanned outages.
US ACE – NW	Agree	
SCE	Disagree	This requirement would require constant updates to the list of BES Subsystems by each Responsible Entity, as any change that "could affect" the BES Subsystems would trigger the requirement for an update. It is unclear that any Reliability Coordinator or Reliability Assurer would have the capability to approve all of the types of engineering evaluations or assessments that could be applied to the virtually infinite number of potential changes. A Responsible Entity must have the opportunity to seek up-front confirmation from its respective Reliability Coordinator or Reliability Assurer in order to verify that its classification of BES Subsystems is correct. It is unclear how this would be accomplished under Requirement R1. Further, the phrase "any change in the electrical system" is too broad. The drafting team should classify quantitative metrics for what is "change". The clarification should be such that it can scale across the different entities in the industry

Organization	Yes or No	Question 4 Comment (Response page 16)
		and across operational environments.
USBR	Disagree	There are three points, the requirement R 1.2 implies that the Reliability coordinator may approve un- documented assessments. The requirement should indicate that the Responsible Entity shall “provide” approved evaluation or assessments. Second, the requirement should be specific to the attachment sections in which the approval is made. Namely Sections 1.1, 1.5, 2.1,and 2.2. Last, there is not requirement for bilateral communication in assessing the impact of assets or cyber systems with the neighboring interconnected responsible entities.
Dyonyx	Agree	
MISO	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. “However, an external reviewer’s role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.”
Westar	Disagree	
Green Country	Disagree	I wish I had a suggestion, BUT the terms "under its ownership" are troublesome. The responsible entities have already been defined as result of registration. To prevent future misunderstanding remove that phrase. Because I can see a harsh interpretation of requiring ownership to compile all its owned generation into a combined MW output and then apply it to table 1 for example
Oregon PUC		The term “engineering evaluation or other assessment method(s)” needs to be better clarified and specified. The standard needs to have clearer and more specific processes for exceptions.
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree with this requirement. In 1.1, the phrase "or any other change in the electric system that could affect the impact" is very vague and would lead to difficulties in demonstrating compliance on the part of registered entities, and assessing compliance on the part of regulating entities. For example, would this vague definition encompass changes made on neighboring systems because they would “affect the impact” of PGE’s system, therefore triggering the reporting requirement? Such a situation would not only be impossible to demonstrate or assess compliance, but also onerous to attempt to track. In 1.2, based on the structure of the sentence, PGE is unclear whether this means every engineering study or evaluation must be approved and such approval documented, or whether it would require using only methodologies approved by the

Organization	Yes or No	Question 4 Comment (Response page 16)
		reliability coordinator.
PSEG	Disagree	Comment #1: Suggested rewrite for Requirement 1: Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…" We suggested in question 1c that the term "BES Subsystem" be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding the SDT expectations. In addition, the term "BES Subsystem" does not align with the terms used in Attachment 1. (Attachment refers to the Generation Subsystem, Transmission Subsystem and Control Center) We believe that the result of this requirement is that each entity has to identify through some naming convention a list of each Generation Subsystem, Transmission Subsystem and Control Centers they own. As we provided under the definition of Transmission Subsystem this will require entities to understand the relationship between their BES Cyber Systems and that could be compromised through the specific BES Cyber System. Examples repeated from Question 1e 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. We believe that our suggestion aligns this requirement to the terms used in Attachment 1. Additional comments about the proposed requirement: What is the goal of this requirement? and What is the requirement asking of Responsible Entities? Is this requirement requiring an entity to make a summary list of all of our Transmission Subsystems (Substation Names) and identify them as either "High", "Medium" or "Low"? Or Is this requirement requiring an entity to make a detailed list all of our Transmission Subsystem including its associated Cyber Assets and identify them as either "High", "Medium" or "Low"? Suggested rewrite for Requirement 1.1: Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. Our proposed goal is clear as to when the update has to occur for big / major changes to an entities system. We believe that the phrase "any other change in the electric system that could affect the impact of BES Subsystems on the BES" should be deleted because it does not provide enough clarity as to what would and would not qualify. As an alternative the SDT should consider adding a new requirement for entities to perform an annual review of its list for

Organization	Yes or No	Question 4 Comment (Response page 16)
		those items which an engineering assessment was performed. An annual review would capture the goal of getting entities to review and if necessary update their list based on changes to their system. Suggested rewrite to Requirement 1.2: Replace Reliability Coordinator or Reliability Assurer with Planning Coordinator. We believe that the Planning Coordinator is the best entity to provide review and feedback on engineering assessments.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI's comments regarding this question. This includes suggested changes to attachment 1. In addition, Wisconsin Electric Power Company feels the 30 day requirement to update is too short and should be extended to quarterly
Idaho Power	Disagree	A more prescriptive description of what an appropriate engineering evaluation or assessment method would be better. As written, the RC will be approving multiple proposals which could lead to inconsistencies in the categorization of subsystems.
SOCO	Disagree	As written, it is not explicitly stated that the listing of cyber systems associated with BES Subsystems listed in R1 is only to be done for the R1 listing for the Entity performing the analysis. This leaves in limbo, for example, the situation where the output from a syncrophasor unit is not used for reliability purposes by an Entity but is used for those purposes by their RTO. The intent that an Entity is only responsible for cyber systems associated with their own BES subsystems should be made explicit. In 1.1, the phrase "any other change in the electric system that could affect the impact" is very nebulous and will be hard to prove compliance to an auditor if "every modification" isn't explicitly studied, documented and approved. Approval by a outside party is required under this Requirement for any engineering evaluation. The Standard identifies the reviewing party as the Reliability Coordinator or Reliability Assurer. This may require that utilities evaluate documentation from neighboring competitors. To accomplish this may require a transfer of potential proprietary and competitive information. Further more it would require that security related information be more widely disseminated to individuals outside the security policy and procedural control of the originating organization. This requirement will present staffing, scheduling and budgeting burdens on the reviewing party to perform evaluations for potentially multiple utilities. The use of engineering evaluations is typically auditable but not subject to a routine outside independent review. The Regulator should consider the development of a review body or allow the use of an independent reviewer it this approach becomes a requirement. Engineering evaluations for some entities may require a seal from a registered professional engineer certified in the State of the installation. This may require that the approvers be registered in numerous States. Suggest that the Reliability Coordinator for the balancing authority approve the engineering studies and list of identified assets for their own balancing authority. They are the most knowledgeable of their own system conditions and planning studies and would be in the best position to understand impacts of assets on their system.

Organization	Yes or No	Question 4 Comment (Response page 16)
DTE	Agree	
AEP	Disagree	Refer to question #2 above.
Edison Mission	Agree	
Calpine	Disagree	New purchased assets may take longer than 30 days to submit a list. We suggest allowing 90 days for new assets.
NS%T	Disagree	We believe impact criteria should be simplified for the sake of inter-Entity and inter-Region consistency. We are concerned about the situation that could arise with sub-requirement 1.2 if a Responsible Entity's assets spanned multiple RCs and the RCs did not agree on the results of engineering evaluations.
Flathead	Disagree	For low impact assets, the 30 day requirement is an unnecessary burden on local distribution entities that currently don't have critical assets, but might under this low impact inclusion. Should be an annual evaluation only. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at LSE/DPs that didn't identify critical assets.
E ON	Disagree	The update should be performed on a by exception basis. In other words, a complete inventorying of all BES Subsystems (high, medium and low) is unnecessary. Only those BES Subsystems that fall into a new category as a result of new or decommissioned facilities should be included in any re-appraisal.
Carthage	Agree	
WECC	Disagree	The determination of criticality should not be required to be validated by the RC's or Reliability Assurer. We do not agree that the RCs are equipped or staffed to perform this function.
Entergy	Disagree	1. Beginning the process using R1 & Attachment I is illogical for addressing this cyber security puzzle, and only obfuscates the issues truly salient to the solution set. 2. R1/Attachment I create a great deal of unnecessary ongoing work and regulatory exposure. 3. Clear delineation of exactly what constitutes a "BES Subsystem" in practice in any number of various scenarios is elusive at best. 4. Is it appropriate to require Reliability Coordinators to accept responsibility for 'approving' and/or 'validating' "engineering or other assessment methods?" If the Reliability Coordinator is found to have been mistaken after the fact, who will be fined? What if the mistake involves Entities whose operation spans more than the aegis of an individual Reliability Coordinator? 5. In practical terms, 30 days is a very narrow time window for what's required.
CenterPoint	Disagree	Disagree – See comments on 1.a. Besides the problems with the proposed new "subsystem" approach, it is unrealistic to perform meaningful on-going engineering evaluations or other assessments with each and every change to the BES,

Organization	Yes or No	Question 4 Comment (Response page 16)
		which is the de facto R1.1 requirement. It is even less realistic to add a new layer of review to this process on an on-going basis as R1.2 requires. Also, R1.2 would require definition of yet another functional entity, “Reliability Assurer”, which will likely cause even more confusion among practitioners trying to implement the new paradigm.
LCRA	Agree	
FRCC	Disagree	In requirement 1.1, the phrase " or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System" is extremely broad and could be almost anything. This would most likely lead to an interpretation request which should be avoided in the development of the requirement. If the drafting team knows what kind of changes would fall in this category they should consider specifically stating them or need to revise to remove the ambiguity in the phrase.
NIPSCO	Disagree	We are concerned with the ability of the RC or the RA to make the determination required in 1.2. Additionally, we would like clarification regarding what the RC or RA is approving; the methodology, the HML categorization of the BES subsystems, or both. Suggestion: Review and discuss with the RC’s and RA’s their position on satisfying this requirement as written. Additionally, clarify the intent of the required RC / RA approval.
ConEd	Agree	
EEI	Disagree	1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability “must run” units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem. 1.5. Each Transmission Subsystem that contains substations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station. 1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) consistent with FAC-10.

Organization	Yes or No	Question 4 Comment (Response page 16)
		1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We believe that 1.9 is duplicative with the presence of 1.1-1.4 and 1.8 We believe that 1.10-1.12 is duplicative with the presence of 1.7 1.13. Each Protection System associated with Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an material adverse reliability impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more …… * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and that functional entity submits a written request for the information. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments. ... 2. BES subsystem with the following characteristics will be determined to be Medium Impact (M) unless it has been determined that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 1,000 MVA or more. 2.2. Each Transmission Subsystem that contains substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or

Organization	Yes or No	Question 4 Comment (Response page 16)
		frequency stability support. 2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. 2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. 2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above. Regarding 1.1, additional clarity is required. A literal reading of 1.1 could require an entity to update its categorized list of BES Subsystems, if there is any change by any entity anywhere on the grid. This could include changes to the grid brought by natural disasters such as ice storms or hurricanes. Consider: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the Responsible Entity commissioning new BES Subsystem(s), decommissioning BES Subsystem(s) or being notified by a transmission planning authority of changes in the electric system that could affect the impact of the Responsible Entity's BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. Regarding 1.2, the industry would be aided by the provision of examples of approved engineering evaluation methods. EEI believes that the standard should either better define an acceptable/minimum engineering evaluation that needs to be performed or specify the ability of individual entities to determine they are allowed to determine the engineering evaluation that they will perform. If the standard is going to specify external review they need to provide some guidance on what the level of review is going to be and the items that need to be considered for the review. EEI is concerned about the designation of Reliability Coordinator or Reliability Assurer as being responsible for this oversight role. The Reliability Coordinator or Reliability Assurer may not have sufficient resources or expertise to satisfy the obligation. It may be more appropriate for the Planning Coordinator and Transmission Planner to perform this task, subject to review.
O&R	Agree	
Alliant	Disagree	R1 needs clarity concerning joint ownership and should be rewritten as follows: " Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 - Criteria for BES Impact Categorization of BES Subsystems. R1.1 needs clarity and should be rewritten as follows: "The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of its commissioning of any new BES Subsystem, its decommissioning of any existing BES Subsystem or its modification of any existing BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days following the completion of the commissioning, decommissioning, or modification.

Organization	Yes or No	Question 4 Comment (Response page 16)
		The term "Reliability Assurer" needs to be defined in the NERC Glossary of Terms.
Ameren	Disagree	Ameren feels that 30 days is too short of time to update the categorized list of BES Subsystems, 90 days would be much more practical. In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved. Requirement R1.2 should be tied to testing of extreme contingencies, such as those described in TPL-004-0. Also, we disagree with the role of Reliability Coordinator as the RC has a time horizon too short for this task per the NERC Functional Model. For this reason, replace Reliability Coordinator with Planning Authority who would work with the Transmission Planner. Also, the role of the Planning Authority should be that of inclusion of additional assets not in evaluation in assessment methodology per the FERC order 706, par 325.
Black Hills	Disagree	Agreement is conditional upon thorough understanding of "ownership". Joint ownership requires understanding who assesses, and if multiply "assessed" whose view prevails. Under CIP-002-1, if two entities jointly owning as asset disagree on criticality, the owner designating as 'critical' prevails. In 1.2, does RC or Regional Assurer approval of assessment method(s) used by the Responsible Entity refer to "approval of the general process" or a specific assessment approval? Further, do both 'evaluations' and 'other 'assessment methods' need to be approved; or just 'other assessment method(s)'?
TNMP	Disagree	TNMP believes the phrase “BES Subsystems under its ownership.” does not handle jointly-owned facilities well. Consider the scenario where Responsible Entity ‘A’ has ownership of 4 breakers and two lines coming into a substation with an operation voltage greater than 300kV and Responsible Entity ‘B’ owns eight additional breakers and four additional lines to the same substation at the same rating. The two Entities separately-owned BES Subsystems are connected by the substation bus. If all the controls for the substation come into a single control house owned by Responsible Entity ‘B’, and the whole station is controlled by Responsible Entity ‘B’ should Responsible Entity ‘A’ be responsible for control house equipment as a result of its ownership of the devices? Another variation on the scenario is each Responsible Entity owning a separate control house for each part that they own and control. Using the criteria in CIP-002 Attachment 1, does Responsible Entity ‘A’ have a BES Subsystem with High or Med BES Impact? The piece Responsible Entity ‘A’ owns only has two transmission lines and two pieces of bus connecting to piece owned Responsible Entity ‘B’. However, the substation as a whole has 6 lines at a voltage level greater than 300 kV. While this second scenario deals more with the content of CIP-002 Attachment 1, it is still an issue that should be resolved in either the wording of Requirement 1 or Attachment 1. Another concern with the proposed requirement is the “or any other change in the electric system that could affect the impact of BES Subsystems” statement. If a change occurred in the system of Responsible Entity ‘A’ that altered the impact on a BES Subsystem in the connected system of Responsible Entity ‘B’ then ‘B’ would be liable for the 30 calendar day clock. Requirement R2 puts the onus upon the Responsible Entity owning a Generation Subsystem to provide information to connected Responsible Entities, which may not have access to the same information. The current

Organization	Yes or No	Question 4 Comment (Response page 16)
		wording of R1 puts the onus upon the Responsible Entity who doesn't have the information to know about the information. In the scenario if Responsible Entity 'A' was to report the change to its Reliability Coordinator or Reliability Assurer then it should be up to the Reliability Coordinator or Reliability Assurer to notify Responsible Entity 'B' that a neighboring change has impacted one or more Transmission Subsystems of Responsible Entity 'B'.
NVEnergy	Disagree	We agree with the concept of the requirement, yet are concerned about two things: the lack of definition round what sort of "other change" that "could affect" the impact on the BES as indicated in 1.1 and the discretion allowed to the Entity to conduct the engineering evaluation or assessment provided in 1.2. It is not clear that the Reliability Coordinator is in the best position to approve that method without having clear guidance and boundaries to promote consistent approaches. While the SDT's efforts appear to attempt to bring some clarity to the characteristics that define the Impact Level (High, Medium, Low), this effort is then unraveled by allowing for an undefined alternative engineering analysis to overturn the initial classification. This would be acceptable if more guidance is provided, perhaps via another attachment, to help the Entities conduct consistent exclusion analyses. We believe there should be more focus placed on the cyber systems themselves, which on an individual basis can impact the BES.
MWDSC	Disagree	Unclear what assessment method will be approved. Recommend having a guideline at the same time as standard is completed such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009. Recommend changing 1.2 to: "The Responsible Entity shall document any engineering evaluation, or in the alternative another assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1." Also, make similar change to M1.2 and Attachments 1.5 and 2.2.
Empire	Disagree	I disagree with the 30 day requirement specified in 1.1. This should be extended to 120 days due to the complexity of these devices and the approvals that could be needed to make these changes.
SWTC	Agree	
SCEG	Agree	
Exelon	Disagree	We are concerned that statement in 1.1 is currently open for inconsistent interpretation and suggest the following revision: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change made by the Responsible Entity that could affect the categorization of the BES Subsystem, within 30 calendar days of the completion of the change. We would ask for more clarification concerning "engineering evaluation" as stated in section 1.2. Specifically the criteria and basis to be used, and to address the possibility that "Responsible Entity" and Reliability Coordinator/Reliability Assurer may for some entities be one and the same.

Organization	Yes or No	Question 4 Comment (Response page 16)
BPA Trans	Disagree	1) There appears to be a void in CIP-002-4. Although stated in the purpose statement, there is no actual requirement statement that the Responsible Entity identify and list their BES Subsystems. CIP-002-4 only requires that those systems be categorized. It seems to assume that identification and listing of the "BES Systems under its ownership" has already occurred. This may not be a big point. However, the original CIP Standards were specific about this part of the process. Note: The guidance document dated December 2009 states that Step 1 of the process is to perform a BES Subsystem Inventory. It continues that "The inventory of BES Subsystems …"and "The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design……." indicating that an inventory of BES Subsystems is necessary. We believe that the first requirement of CIP-002-4 should be the initial identification of BES Subsystems with the appropriate stated criteria/functions etc. Starting the CIP with a requirement to "categorize" assumes that the Subsystems themselves have already been identified. The text provided below is suggested as an example of a potential new R1 to "inventory/identify" BES Subsystems. R1. The Responsible Entity shall create an inventory of all BES subsystems owned by the entity, including all: Generation Subsystems, Transmission Subsystems, and Control Centers. R1.1 The Responsible Entity shall base its inventory on the list of Functions Critical to the Reliable Operation of the Bulk electric System (CIP-002-4 Attachment 2) R1.2 The Responsible Entity should consider any associated BES Cyber Systems when performing the inventory and defining the boundaries of BES Subsystems. Note: R1.1 and R1.2 are taken directly from the December 2009 guidance document. With the addition of new requirement #1, existing R1 becomes R2. It is edited for clarity: R2. The Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. (Violation Risk Factor: High) R2.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. R2.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1. Additionally, no criteria is provided for the identification of BES Subsystems other than "Generation Subsystems, Transmission Subsystems and Control Center." Are there others?
HQT	Disagree	RC should be removed from 1.2.

Organization	Yes or No	Question 4 Comment (Response page 16)
Allegheny Energy	Agree	We support requirement 1.1 as it is an extension of the current CIP-002 version 1. We are concerned with the ability of the Reliability Coordinator to make the determination required in 1.2.
KCPL	Disagree	I am concerned regarding the potential flood of requests to the Reliability Coordinator(s) that could result from Requirement 1.2 with the criteria proposed here under Attachments 1 and 2. I believe appropriate criteria may substantially stem requests to the RC.
Connectiv Energy	Agree	
MidAmerican	Disagree	CIP-002-4 as proposed requires all BES facilities to be in CIP scope. It thereby addresses the criticism that entities did not include enough facilities. MidAmerican supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all operated BES facilities: transmission substations and generation resources connected at 100 kV and above and transmission control centers that are subject to other existing NERC standards. This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards. However, categorization level determinations should be addressed in the security control standards. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. Further, if engineering evaluations are required in some cases as drafted in CIP-002-4, the prescription to update documentation within 30 days of a change in the BES is not realistic.
CPG	Disagree	R1.1 would require monthly reviews of all assets to ensure that no changes have been made, and that if there were any changes, they would have to be documented. Changing this requirement to quarterly reviews would allow for a more thorough investigation of any changes and allow time for those changes to be well documented. R1.2 would require the Reliability Coordinator to approve all engineering evaluations (or other methods) to support the categorization of BES Subsystems. If a Generator Owner/Operator concurs with engineering assessments shared with its connected Transmission Owner/Operator, then that assessment would ensure proper coordination and categorization of BES Subsystems. Having it then approved by the Reliability Coordinator adds another cumbersome and unnecessary level of approval. A definition or clarification as to what is meant by the "Reliability Assurer" is also needed.
Santee Cooper	Disagree	Still do not believe the BES Subsystem classification is clear in achieving the overall objective of the new Standard.

Organization	Yes or No	Question 4 Comment (Response page 16)
OGE	Disagree	• Should dual-ownership of BES subsystems be addressed in this document? • The phrase "any other change in the electric system that could affect the impact…" is excessively open-ended. Needs to be a change that could increase the impact rating. • Is 1.2 indicating that the RE shall have the RC approve their engineering evaluation and/or assessment method(s) or should the RE document that it is using an RC approved engineering evaluation and/or assessment method(s)?- • SDT should extend the time period for updating the list and ultimately asset compliance to 90 days or greater.
Oncor	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose the following: Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems.
PPL Supply	Disagree	A more precise definition of Black Start generating units is needed that in the proposed Rev. 4 or the EEI comments. To say that "Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem." is inadequate to identify only those generating units that are used for initial restoration of the BES. System restoration plans normally identify all units from the blackstart initiating through the thermal generation at the end of the cranking path, including any intermediary units, so clarification is needed to avoid misinterpretation.
St. George	Agree	
NGRID	Disagree	The use of "BES Subsystems" is not consistent with the terms used in Attachment 1 and should be replaced by the specific terms such as Transmission/ Generation subsystems.
MGE	Disagree	Do not agree with the following: The BES Subsystem definition is not required and should be removed since Generation Subsystem, Transmission Subsystem, and Control Center are clearly defined. R1, "As a step in identifying appropriate security controls for its assets" should be deleted; the statement does not add content or instruction to the requirement. R1.1, "or any other change in the electric system" should be removed because it does not provide enough clarity and could be interpreted to mean just about anything. R1.2, Reliability Assurer is not defined by NERC. Please provide a definition. And it is not listed in the Applicability section, please add. R1.2, As written the RC or RA (?) will have to approve all engineering evaluations or other assessment methods to support categorization of BES Subsystems where required by Attachment 1. What is the basis of electing the RC or RA to have the authority to approve a methodology concerning a BES Subsystem of an entity other than that entity? To

Organization	Yes or No	Question 4 Comment (Response page 16)
		reduce any risk associated with categorizing of a BES Subsystem, the RC or RA will simple not approve any type of evaluation, ever. There are no other requirements or proposed guide lines to assist in the evaluation that the RC or RA will use in approving the categorization of BES Subsystems. Order 706 paragraph 325 states "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets." If this was added to reduce what we now know as TFE's, it does not. Paragraph continues with "We recognize, however, that there may be a legitimate reason for a responsible entity to dispute such a determination, possibly through an appeal. We leave it to the ERO to determine the need for such an appeal mechanism and, if appropriate, the development of appropriate procedures (or reliance on appeal procedures currently provided in the NERC Rules of Procedure). While the ERO may determine that an appeals process is a necessary aspect of this program, we do not believe that the burden of such appeals outweighs the benefits of the external review of critical asset lists". Recommend R1.2 be deleted in its entirety.
FE	Disagree	In general we do not support the categorization described by the R1 and Attachment 1 as described in our prior comments. However, we offer the following comments: 1. Item 1.1: The team should consider a separate requirement for this such that a Lower VRF can be applied. Merely updating a list within 30 days is a documentation item that should not be subject to a High VRF penalty. 2. Item 1.2: FE believes that the need for RC or RA approval can be avoided by requiring the study follow the PC's Methodology for identifying IROL as defined in FAC-010/FAC-014. Furthermore, we do not support the use of the RA. The RA is a Functional Model Guideline (which we did not support) and the NERC registration criteria for responsible entities do not support the RA classification.
TECO	Disagree	Reliability Assurer is capitalized but not otherwise defined. Reliability Assurer does not appear in the FERC approved Glossary of Terms nor in the Functional Model. This position is unclear and should be removed. We support the EEI comments regarding attachment 1 and offer additional clarification for items 1.2, 1.4 and 2.2. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of either the Responsible Entity's Contingency Reserve obligation or if the Entity is part of a Reserve Sharing Group, the Reserve Sharing Group's Contingency Reserve obligation. 1.4. Each Transmission Subsystem comprising the Cranking Paths and each Blackstart Generation Subsystem that has been included in the regional system restoration plan. 2.2. Each Transmission Subsystem that contains substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines connected to the station.
CECD	Disagree	1. "As a step in identifying appropriate security controls for its assets" should be deleted because the Purpose of the standard has already been stated.

Organization	Yes or No	Question 4 Comment (Response page 16)
		2. What qualifies as an engineering evaluation? (3) The requirement should explicitly indicate that a dated list and categorization of BES subsystems is necessary for compliance as indicated in the relevant measurement.
MRO	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose the following: Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. We feel R1.1 is ambiguous as written, and would propose the following: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of its commissioning of any new BES Subsystem, its decommissioning of any existing BES Subsystem or its modification of any existing BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days following the completion of the commissioning, decommissioning, or modification. We also feel the term "Reliability Assurer" should be defined in the NERC Glossary of Terms.
GTC	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing "within 30 calendar days of the completion of the change" with "within 30 calendar days of the Responsible Entity becoming aware that the change has occurred". Also, to clarify applicability, we suggest replacing the phrase "that could affect the impact of BES Subsystems" with "that could affect the degree of impact of the Responsible Entity's BES Subsystems." For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
Xcel	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. We believe 30 days is too short and suggest 90 days is more appropriate.
BGE	Disagree	We do not agree with this requirement and suggest changes to Attachment 1 as detailed in our response to Item #3. The exact start time for the 30 day clock needs clarification. Work could be completed in stages, for example: BES Subsystem work may incorporate new equipment brought on-line in stages. Is the "completion of the change" defined as completion of each individual stage or the entire project? Particularly important, is the relationship of system protection work to the completion of the entire project, that is, system protection work may be completed and in service before equipment is energized. The term "Reliability Assurer" needs to be fully defined. According to the NERC "Reliability Functional Model Technical Document", version 5, December 2009, the specific role of the Reliability Assurer is not fully developed at the present

Organization	Yes or No	Question 4 Comment (Response page 16)
		time. The approval criteria used by the Reliability Coordinator or Reliability Assurer is not defined.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Has the drafting team coordinated with all registered Reliability Coordinators (RC)on how they will handle this? Or confirmed that they are ready to handle these requests? Also, who would be the Reliability Assurer (RA)? This does appear to be a FERC approved registration criteria yet. The role of the RA in Version 4 of CIP-002 is critical, there should be a better understanding of who or what type of organization will perform this activity. Also, in the provision that either the Reliability Assurer or the Reliability Coordinator may approve the engineering assessment as stipulated in Requirement 1.2, there should only be one option either the RA or the RC but not both. We feel that the drafting team needs to coordinate with all of the registered Reliability Coordinators and/or their agents to confirm that they are prepared to handle requests for validating engineering assessments. There should be language within the standard that holds the RC to be required to perform this task from a mandatory compliance standpoint.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP suggested in question 1c that the term “BES Subsystem” be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding of the SDT expectations. In addition, the term “BES Subsystem” does not align with the terms used in Attachment 1.
FMPA	Disagree	As described earlier, the addition of the concept of Subsystem is unnecessary and adds ambiguity and complexity. The requirement would be much improved by simply replacing Subsystem with Cyber System. Bullet 1.1 could be modified to include commissioning or decommissioning of any Facility or BES Cyber System. Also, the use of the term “assets” adds ambiguity. The only security controls envisioned are for Cyber Systems, so, use the term Cyber Systems.
Duke	Disagree	We disagree with the approach of categorizing BES Subsystems and instead prefer the alternative “Cyber First” approach. Also, we disagree with making the Reliability Coordinator responsible for approving engineering or other assessment methods used to categorize BES Subsystems, because the Reliability Coordinator does not have this capability or resources.
NBSO	Disagree	1.2 is not clear. Attachment 1 should allow for more stringent RC input. The RC should not be used for entities to get exemptions from high impact level.
AESI	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing “within 30 calendar days of the completion of the change” with “within 30 calendar days of the Responsible Entity becoming aware that the change has occurred”. Also, to clarify applicability, we suggest

Organization	Yes or No	Question 4 Comment (Response page 16)
		replacing the phrase "that could affect the impact of BES Subsystems" with "that could affect the degree of impact of the Responsible Entity's BES Subsystems." For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
IESO	Disagree	In concurrence with the IRC we submit the same response as follows: At the CIP-002-4 Webinar, the Standard Drafting Team invited comments/suggestions on how best to address "third party review", as is required by Order No. 706 (and 706-A). See Presentation at Slide 10. We appreciate the SDT inviting comments on other approaches to addressing Order No. 706's requirement that there be some external-party review of Responsible Entity's lists of those assets designated as critical, and potentially requiring critical infrastructure protections. In its presentation, the SDT discussed the need to respond to Paragraph 322 in Order No. 706; the comments below discuss Paragraph 322 and other relevant paragraphs in Order No. 706 and 706-A. These comments also pertain primarily to the US-based registered entities, because some Canadian Entities have different oversight authority/enforcement responsibility than their US-based counterparts. First, and foremost, the matter of third-party review should be handled through the NERC Rules of Procedure/CMEP, and not in the Standard Requirements. The key parts of Order No. 706 (and 706-A) set out three (3) principles. (II) Responsible entities are, and should remain, responsible for identifying their own assets as requiring critical infrastructure protection. The SDT makes clear in the plain language of the Standard that Responsible Entities are responsible for their own assets. Paragraph 328 of Order No. 706 states that: "responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large – in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility." See also Order No. 706-A at P53 (: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity. The fact that the Commission has directed the ERO to develop an external review process – as a backup to help assure that the responsible entity does not overlook any critical assets – does not shift this responsibility from the responsible entity to whatever entity conducts the external review.") (III) NERC and the Regions should issue guidance to Responsible Entities that do not have a "wide-area" view in

Organization	Yes or No	Question 4 Comment (Response page 16)
		order to assist them in identifying which of their assets required critical infrastructure protection (Order No. 706 at P322). The SDT had provided guidance in the form of the Standard itself – i.e., Attachment 1. This Draft Standard effectively directs Registered Entities on how to classify their assets. (IV) External review is necessary to: (a) help identify trends in the industry (Order No. 706 at P322 and to support consistency (Id.), and is necessary to review asset more frequently than would occur through the regular audit cycle. (Order No. 706 at P324) (FERC "does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations"). With regard to Principle III, FERC explained that NERC may choose to "designate" a Registered Entities (such as, but not necessarily, a Reliability Coordinator) as responsible for this external review if NERC/Regional Entities determined that they did not have the resources/expertise to conduct this review. (Order No. 706 at P255)("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). In Order No. 706-A, FERC added that if NERC designated a Reliability Coordinator as having oversight/review authority, the Reliability Coordinator should have the same liability protections as NERC. (Order No. 706-A at P53). In drafting CIP-002-4, the SDT therefore largely adhered to the first two principles. The draft language in R1.2 confuses the Principle III, and therefore takes a wrong approach to addressing the Commission's concerns in Order No. 706. With regard to Principle III, the need for more frequent external review than that provided by audits can and should be handled outside of the Standard Development Process. For example, NERC and the Regions can establish spot-checks or off-site audits through the CMEP program, and NERC can require Responsible Entities to submit information to it (or the Regions) through an information request developed under its Rules of Procedure. If the SDT and NERC address the role of third party review through NERC's administration of its Rules of Procedures, many significant problems with R1.2 would be eliminated. These problems are summarized below. First, because NERC would register Regional Entities as "Reliability Assurers", the manner in which Regional Entities would carry out its oversight task should be handled through NERC/FERC review or audit of Regional Entities' adherence to their Delegation Agreements. This would be a better approach to checking on the Regional Entities' performance in providing external review then through an Enforcement Audit process. Second, it is premature to place "Reliability Coordinators" in the Standard. Because NERC has not found that it lacks sufficient resources to take on the external review responsibility, and thereby has not "designated" any other type of Registered Entity with this responsibility, it is premature for the Standard to make reference to the Reliability Coordinator. See Order No. 706 at P255 ("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes

Organization	Yes or No	Question 4 Comment (Response page 16)
		that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). If the Standard Drafting Team is committed to including in its Standard reference to a Registered Entity as having external review oversight, it should wait until NERC makes its designation. Third, assigning external review responsibilities to the Regional Entities (as Reliability Assurers) would facilitate achieving FERC's goal of consistency. Because NERC and the Regional Entities work closely as part of their Regional Entity Delegation Agreement, and because there are fewer Regional Entities than Reliability Coordinators, achieving consistency will be easier if the Reliability Assurers (i.e., Regional Entities) have the external oversight responsibility. Fourth, even if NERC "designates" a Registered Entity (such as, perhaps, a Reliability Coordinator) as having a role in providing external review, the Registered Entity would have the same liability protections as NERC, the Registered Entity is essentially carrying out this role as a NERC-designee. It is easier to capture the roles, responsibilities and liabilities protections through amendment to the Delegation Agreements and Rules of Procedure. In Order No. 706-A, FERC reaffirmed the protections given to external reviewers. See Order No. 706-A at P53 (""we agree [with the ISO/RTO Council] that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself."). These protections include no finding of liability unless intentional misconduct or gross negligence is found. See, e.g., Bylaws at Section 3 (NERC's trustees, officers, employees, and agents are held harmless "for any injury or damage to [any NERC Member] caused by any act or omission of any trustee, officer, employee, agent, or volunteer in the course of performance of his or her duties on behalf of the Corporation, other than for acts of gross negligence, intentional misconduct, or a breach of confidentiality"). Fifth, the combination of R.1.2 and 1.1. and 1.5 in Attachment 1 appears to require an external review by the Reliability Assurer or Reliability Coordinator to exclude assets. This exclusion is contrary to the type of external review identified in Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets." Clearly the Commission intended to add facilities to the critical assets not exclude them with the external review. R1.2 does not explicitly describe the nature of the third party review, we interpret the Draft Requirement to not require a Reliability Coordinator/Reliability Assurer to conduct such reviews and/or issue approvals. Clarity could be useful, because others interpret the Standard to require an exception-type external review – i.e., when a Registered Entity does an engineering evaluation that claims that its assets should be classified according to Attachment 1. Others have interpreted the language to require external review of all entities to determine whether they are leaving out assets from their lists. Sixth, even if the R1.2 is meant only to apply to an external reviewer doing "exception-type" reviews, including this role in the Standards suggests that so long as a Responsible Entity does any type of engineering evaluation, the Responsible

Organization	Yes or No	Question 4 Comment (Response page 16)
		Entity can effectively shift responsibility to the external reviewer. Because there is no sanction for incomplete or non-substantive evaluations, the External Reviewers may be deluged with requests to "exempt" assets from the Attachment 1 categorization. This language would effectively undermine FERC's direction that Responsible Entities remain responsible for classifying their assets and they cannot shift this responsible to the Regional Entity or another Organization. See Order No. 706 at P328. In sum, the SRC recognizes that a different set of expectations may apply to those Regional Entities that are also Reliability Coordinators (e.g., WECC). These entities already have liability protections per their NERC delegation agreements, and in their role as Regional Entities, they ultimately have authority over whether the Responsible Entity has correctly identified bulk power system assets as subject to critical infrastructure protection. Similarly, some of the Canadian Reliability Coordinators (e.g., IESO through its enforcement group) exercise similar oversight authority as a Regional Entity with regard to other Registered Entities. While we don't think the nature of this third-party review should be discussed in the standard itself, if the SDT wants to continue to refer to it in the Standard, at this point, the Standard should only refer to Reliability Assurers.
Manitoba 2	Disagree	What is the purpose of this requirement? Does it imply that the security controls are in place and this is just final documentation? If so, there should be separate requirements with different VRFs (low for the paperwork). Completing the implementation of the security controls would be a High VRF. Please define "any other change in the electric system" as it applies in this definition. Does this scope include the entire electric system across the continent, across the region, or across the Responsible Entity's territory? Please define what is meant by "completion of the change" as it applies to this definition. The statement " … affect the impact of the BES Subsystem …" should be revised to "… change the impact categorization level of the BES Subsystem…", which requires the documentation to reflect the changes in categorization, not all the changes in the electric system. We do not feel that 3rd party oversight or approval is required, since the Responsible Entity is responsible for conducting its engineering evaluation with due diligence. The direction of the standard, to include all BES Cyber Systems in the categorization, will mean that security controls will be specified for BES Cyber Systems with a categorization of low. Any such identified security controls will then also be auditable. All BES Cyber Systems are not critical to support a BES Subsystem, and as such should not require auditable security controls. Guidance provided to industry on security controls for low impact BES Cyber Systems would be sufficient for the necessary strategic direction and would not require external audit of these low impact security controls. Low impact BES Cyber Systems should not be listed or be required to be auditable in the standard. Including the low impact BES Cyber Systems will significantly increase the implementation timeframe, increase the cost and will divert resources required to implement the controls associated higher impact levels. Auditable security controls in CIP-003 through CIP-009 should only be applied to high impact and medium impact BES Cyber Subsystems.

Organization	Yes or No	Question 4 Comment (Response page 16)
ATC	Disagree	Suggested rewrite for Requirement 1: Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…" ATC suggested in question 1c that the term "BES Subsystem" be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding the SDT expectations. In addition, the term "BES Subsystem" does not align with the terms used in Attachment 1. (Attachment refers to the Generation Subsystem, Transmission Subsystem and Control Center) We believe that the result of this requirement is that each entity has to identify through some naming convention a list of each Generation Subsystem, Transmission Subsystem and Control Centers they own. As we provided under the definition of Transmission Subsystem this will require entities to understand the relationship between their BES Cyber Systems and that could be compromised through the specific BES Cyber System. Examples repeated from Question 1e 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. We believe that our suggestion aligns this requirement to the terms used in Attachment 1. Additional comments about the proposed requirement: What is the goal of this requirement? and What is the requirement asking of Responsible Entities? Is this requirement requiring an entity to make a summary list of all of our Transmission Subsystems (Substation Names) and identify them as either "High", "Medium" or "Low"? Or Is this requirement requiring an entity to make a detailed list all of our Transmission Subsystem including its associated Cyber Assets and identify them as either "High", "Medium" or "Low"? Suggested rewrite for Requirement 1.1: Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. Our proposed goal is clear as to when the update has to occur for big / major changes to an entities system. ATC believes that the phrase "any other change in the electric system that could affect the impact of BES Subsystems on the BES" should be deleted because it does not provide enough clarity as to what would and would not qualify. As an alternative the SDT should consider adding a new requirement for entities to perform an annual review of its list for those items which an engineering assessment was performed. An annual review would capture the goal of getting entities to review and if necessary update their list based on changes to their system.

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 4 Comment (Response page 16)</th></tr>
<tr><td></td><td></td><td>Suggested rewrite to Requirement 1.2:
Replace Reliability Coordinator or Reliability Assurer with Planning Coordinator.
ATC believes that the Planning Coordinator is the best entity to provide review and feedback on engineering assessments.</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 4 Comment (Response page 16)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>It is unclear what "appropriate" means. There should be care in adding descriptive words that are open to interpretation and for which no specificity is provided.
R1.1 requires that the categorization must be updated when “….any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System. However it is unclear whether these are permanent changes or could include temporary changes such as extended outages. It is also unclear whether changes caused by adjacent interconnections that could affect the impact of another’s BES Subsystem are included in this requirement. Because of these concerns the updated within 30 days may be too short.
It is unclear what criteria the RC or RA will use in approving an assessment method in order to ensure consistency as well as timeliness.
Puget Sound Energy strongly supports the language defined by EEI in response to this question.
Relative to Attachment 1 it is unclear what is the technical justification for using 2,000 MW and 1,000 MW for thresholds of high and medium.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA recommends changing “ownership” to “operation”.
In 1.1, IMPA recommends changing the time from 30 calendar days to 60 calendar days to allow utilities more time.
The usage of “any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System” is ambiguous and subjective. IMPA recommends using the words “any change in the BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System”.
For 1.2, a standard engineering evaluation or other asset method should be developed so the Reliability Coordinators or Reliability Assurers across the country can be consistent or at the very least the regional engineering evaluations should</td></tr>
</table>

Organization	Yes or No	Question 4 Comment (Response page 16)
		be consistent. In addition, IMPA believes that performing an engineering evaluation or other asset method could be a financial burden on smaller entities that do not have the in-house expertise to perform these evaluations. Therefore, IMPA would like the SDT to consider the use of the prevailing practices of utilities in the region who have performed the engineering evaluations to support the categorization as an acceptable alternative.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO and ISO-NE comments. Further, it would be necessary for a Reliability Coordinator to have a guarantee of safe harbor and indemnity on approval of evaluations and assessments. It should be made clear that the categorization and subsequent protection of assets is the sole responsibility of the asset owner. That responsibility should not ever be abrogated to any other party. Midwest ISO Comments: We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets."
PacifiCorp	Disagree	- CIP-002-4 as proposed requires all BES facilities to be considered as part of the CIP requirements. It thereby addresses the criticism that entities did not include enough facilities. PacifiCorp supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all operated BES facilities. - This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards. However, categorization level determinations should be addressed in the security control standards. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, PacifiCorp proposes that the development of Attachment 1's concepts be concurrent with the security controls work. - Further, if engineering evaluations are required in order to categorize all BES Subsystems, the requirement to update documentation within 30 days of any changes to any BES Subsystem is not realistic.
IRC	Disagree	At the CIP-002-4 Webinar, the Standard Drafting Team invited comments/suggestions on how best to address "third party review", as is required by Order No. 706 (and 706-A). See Presentation at Slide 10. We appreciate the SDT inviting comments on other approaches to addressing Order No. 706's requirement that there be some external-party review of

Organization	Yes or No	Question 4 Comment (Response page 16)
		Responsible Entity's lists of those assets designated as critical, and potentially requiring critical infrastructure protections. In its presentation, the SDT discussed the need to respond to Paragraph 322 in Order No. 706; the comments below discuss Paragraph 322 and other relevant paragraphs in Order No. 706 and 706-A. These comments also pertain primarily to the US-based registered entities, because some Canadian Entities have different oversight authority/enforcement responsibility than their US-based counterparts. First, and foremost, the matter of third-party review should be handled through the NERC Rules of Procedure/CMEP, and not in the Standard Requirements. The key parts of Order No. 706 (and 706-A) set out three (3) principles. (I) Responsible entities are, and should remain, responsible for identifying their own assets as requiring critical infrastructure protection. The SDT makes clear in the plain language of the Standard that Responsible Entities are responsible for their own assets. Paragraph 328 of Order No. 706 states that: "responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large – in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility." See also Order No. 706-A at P53 (: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity. The fact that the Commission has directed the ERO to develop an external review process – as a backup to help assure that the responsible entity does not overlook any critical assets – does not shift this responsibility from the responsible entity to whatever entity conducts the external review.") (II) NERC and the Regions should issue guidance to Responsible Entities that do not have a "wide-area" view in order to assist them in identifying which of their assets required critical infrastructure protection (Order No. 706 at P322). The SDT had provided guidance in the form of the Standard itself – i.e., Attachment 1. This Draft Standard effectively directs Registered Entities on how to classify their assets. (III) External review is necessary to: (a) help identify trends in the industry (Order No. 706 at P322 and to support consistency (Id.), and is necessary to review asset more frequently than would occur through the regular audit cycle. (Order No. 706 at P324) (FERC "does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations"). With regard to Principle III, FERC explained that NERC may choose to "designate" a Registered Entities (such as, but not necessarily, a Reliability Coordinator) as responsible for this external review if NERC/Regional Entities determined that they did not have the resources/expertise to conduct this review. (Order No. 706 at P255)("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue

Organization	Yes or No	Question 4 Comment (Response page 16)
		burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). In Order No. 706-A, FERC added that if NERC designated a Reliability Coordinator as having oversight/review authority, the Reliability Coordinator should have the same liability protections as NERC. (Order No. 706-A at P53). In drafting CIP-002-4, the SDT therefore largely adhered to the first two principles. The draft language in R1.2 confuses the Principle III, and therefore takes a wrong approach to addressing the Commission's concerns in Order No. 706. With regard to Principle III, the need for more frequent external review than that provided by audits can and should be handled outside of the Standard Development Process. For example, NERC and the Regions can establish spot-checks or off-site audits through the CMEP program, and NERC can require Responsible Entities to submit information to it (or the Regions) through an information request developed under its Rules of Procedure. If the SDT and NERC address the role of third party review through NERC's administration of its Rules of Procedures, many significant problems with R1.2 would be eliminated. These problems are summarized below. First, because NERC would register Regional Entities as "Reliability Assurers", the manner in which Regional Entities would carry out its oversight task should be handled through NERC/FERC review or audit of Regional Entities' adherence to their Delegation Agreements. This would be a better approach to checking on the Regional Entities' performance in providing external review then through an Enforcement Audit process. Second, it is premature to place "Reliability Coordinators" in the Standard. Because NERC has not found that it lacks sufficient resources to take on the external review responsibility, and thereby has not "designated" any other type of Registered Entity with this responsibility, it is premature for the Standard to make reference to the Reliability Coordinator. See Order No. 706 at P255 ("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). If the Standard Drafting Team is committed to including in its Standard reference to a Registered Entity as having external review oversight, it should wait until NERC makes its designation. Third, assigning external review responsibilities to the Regional Entities (as Reliability Assurers) would facilitate achieving FERC's goal of consistency. Because NERC and the Regional Entities work closely as part of their Regional Entity Delegation Agreement, and because there are fewer Regional Entities than Reliability Coordinators, achieving consistency will be easier if the Reliability Assurers (i.e., Regional Entities) have the external oversight responsibility.

Organization	Yes or No	Question 4 Comment (Response page 16)
		Fourth, even if NERC "designates" a Registered Entity (such as, perhaps, a Reliability Coordinator) as having a role in providing external review, the Registered Entity would have the same liability protections as NERC, the Registered Entity is essentially carrying out this role as a NERC-designee. It is easier to capture the roles, responsibilities and liabilities protections through amendment to the Delegation Agreements and Rules of Procedure. In Order No. 706-A, FERC reaffirmed the protections given to external reviewers. See Order No. 706-A at P53 (""we agree [with the ISO/RTO Council] that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself."). These protections include no finding of liability unless intentional misconduct or gross negligence is found. See, e.g., Bylaws at Section 3 (NERC's trustees, officers, employees, and agents are held harmless "for any injury or damage to [any NERC Member] caused by any act or omission of any trustee, officer, employee, agent, or volunteer in the course of performance of his or her duties on behalf of the Corporation, other than for acts of gross negligence, intentional misconduct, or a breach of confidentiality"). Fifth, the combination of R.1.2 and 1.1. and 1.5 in Attachment 1 appears to require an external review by the Reliability Assurer or Reliability Coordinator to exclude assets. This exclusion is contrary to the type of external review identified in Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets." Clearly the Commission intended to add facilities to the critical assets not exclude them with the external review. does not explicitly describe the nature of the third party review, we interpret the Draft Requirement to not require a Reliability Coordinator/Reliability Assurer to conduct such reviews and/or issue approvals. Clarity could be useful, because others interpret the Standard to require an exception-type external review – i.e., when a Registered Entity does an engineering evaluation that claims that its assets should be classified according to Attachment 1. Others have interpreted the language to require external review of all entities to determine whether they are leaving out assets from their lists. Sixth, even if the R1.2 is meant only to apply to an external reviewer doing "exception-type" reviews, including this role in the Standards suggests that so long as a Responsible Entity does any type of engineering evaluation, the Responsible Entity can effectively shift responsibility to the external reviewer. Because there is no sanction for incomplete or non-substantive evaluations, the External Reviewers may be deluged with requests to "exempt" assets from the Attachment 1 categorization. This language would effectively undermine FERC's direction that Responsible Entities remain responsible for classifying their assets and they cannot shift this responsible to the Regional Entity or another Organization. See Order No. 706 at P328. In sum, the SRC recognizes that a different set of expectations may apply to those Regional Entities that are also Reliability Coordinators (e.g., WECC). These entities already have liability protections per their NERC delegation agreements, and in their role as Regional Entities, they ultimately have authority over whether the Responsible Entity has correctly identified bulk power system assets as subject to critical infrastructure protection. Similarly, some of the Canadian Reliability Coordinators (e.g., IESO through its enforcement group) exercise similar oversight authority as a Regional Entity with regard to other Registered Entities.

Organization	Yes or No	Question 4 Comment (Response page 16)
		While we don't think the nature of this third-party review should be discussed in the standard itself, if the SDT wants to continue to refer to it in the Standard, at this point, the Standard should only refer to Reliability Assurers.
PEPCO	Disagree	If the SDT believes that the big iron approach is the better option, we offer the following comments: Please see below amended Attachment 1. 1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined (DELETE not to be essential to the reliability of the BES) that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability "must run" units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. (DELETE Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan.) Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem. 1.5. Each Transmission Subsystem that contains (DELETE switching stations substations) operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines (DELETE leaving connected to the station. 1.6. (DELETE Each Transmission Subsystem comprising the Cranking Paths.) 1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) (DELETE or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method) consistent with FAC-10. 1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We believe that 1.9 is duplicative with the presence of 1.1-1.4 and 1.8 1.9. (DELETE Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above.) We believe that 1.10-1.12 is duplicative with the presence of 1.7 1.10. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would

Organization	Yes or No	Question 4 Comment (Response page 16)
		result in voltage collapse as determined through an engineering evaluation or other assessment method.) 1.11. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. 1.12. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages.) 1.13. Each Protection System associated with Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an material adverse reliability impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more ……. * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and that functional entity submits a written request for the information. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments. 2. BES subsystem with the following characteristics will be determined to be Medium Impact (M) unless it has been determined (DELETE not to be essential to the reliability of the BES) that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 1,000 MVA or more. 2.2. Each Transmission Subsystem that contains (DELETE switching) substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or

Organization	Yes or No	Question 4 Comment (Response page 16)
		frequency stability support. 2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. 2.4. (DELETE Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001-1 for Medium Impact Nuclear facilities as determined under Criterion 2.1 above.) 2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. 2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above. Regarding 1.1, additional clarity is required. A literal reading of 1.1 could require an entity to update its categorized list of BES Subsystems, if there is any change by any entity anywhere on the grid. This could include changes to the grid brought by natural disasters such as ice storms or hurricanes. Consider: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the Responsible Entity commissioning new BES Subsystem(s), decommissioning BES Subsystem(s) or being notified by a transmission planning authority of changes in the electric system that could affect the impact of the Responsible Entity's BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. Regarding 1.2, the industry would be aided by the provision of examples of approved engineering evaluation methods. We believe that the standard should either better define an acceptable/minimum engineering evaluation that needs to be performed or specify the ability of individual entities to determine they are allowed to determine the engineering evaluation that they will perform. If the standard is going to specify external review they need to provide some guidance on what the level of review is going to be and the items that need to be considered for the review. We are concerned about the designation of Reliability Assurer as being responsible for this oversight role. The Reliability Assurer may not have sufficient resources or expertise to satisfy the obligation. It may be more appropriate for the Planning Coordinator and Transmission Planner to perform this task, subject to review.
NEI	Disagree	A) Beginning the process using R1 & Attachment I is illogical for addressing this cyber security puzzle, and only obfuscates the issues truly salient to the solution set. B) R1/Attachment I create a great deal of unnecessary ongoing work and regulatory exposure. C) Clear delineation of exactly what constitutes a "BES Subsystem" in practice in any number of various scenarios is elusive at best. D) Is it appropriate to require Reliability Coordinators to accept responsibility for 'approving' and/or 'validating' "engineering or other assessment methods?" If the Reliability Coordinator is found to have been mistaken after the

Organization	Yes or No	Question 4 Comment (Response page 16)
		fact, who will be accountable? What if the mistake involves Entities whose operation spans more than the aegis of an individual Reliability Coordinator? Frequently from a generator owner/operator perspective they don't know the impacts without contacting the Transmission Owner. Where either the Reliability Coordinator/Reliability Assurer is used for the evaluation, who reviews? Do we have a need for an Independent Third Party Review? In this case, the Reliability Coordinator/Reliability Assurer needs to provide acceptable evaluation methodology E) In practical terms, 30 days is a very narrow time window for what's required. F) Is the expectation that the engineering evaluation is in place at T=0, is there an exclusion timeframe to enable the evaluation to be performed and approved? G) Item 1.1: The team should consider a separate requirement for this such that a Lower VRF can be applied. Merely updating a list within 30 days is a documentation item that should not be subject to a High VRF penalty. H) Item 1.2: NEI believes that the need for RC or RA approval can be avoided by requiring the study follow the PC's Methodology for identifying IROL as defined in FAC-010/FAC-014. Furthermore, we do not support the use of the RA. The RA is a Functional Model Guideline (which we did not support) and the NERC registration criteria for responsible entities do not support the RA classification. I) I) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)

2.2 The Responsible Entity name

2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Organization	Yes or No	Question 5 Comment (Response page 17)
Progress Energy	Disagree	Add a new bullet "2.4 Basis for categorization change." NERC needs to better define or explain "directly interconnected". NERC needs to have CIP-003 through -009 Version 4 defined before we can commit to "within 30 calendar days of developing or updating its BES impact categorization."
Dynegy	Agree	
GSOC/OPC	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2. We suggest changing "Transmission Subsystem owners" to "Transmission Subsystem owners and operators."
Hayden	Agree	I would also suggest that the information also include a) method of notification, b) date of notification
SDGE	Disagree	Transmission Subsystem owners must have input on categorizing the impact that a Generation Subsystem will have on the transmission system; in many cases, the Generation Owners / Operators don't have access to the appropriate

Organization	Yes or No	Question 5 Comment (Response page 17)
		engineering data to make such a determination. With all of the effort required to gather this data and analyze it thoroughly, 30 days may not be enough time. This time period includes the time required to gather data, perform studies and then get approval from the Reliability Coordinator. We propose a 30 day timeframe for providing the results and analysis to the RC. What is the definition of "accurate information"? Need clarification on ownership of generation subsystems; does this mean that this Requirement is not applicable for non-company owned generation subsystems? Need guidance on compliance for company-owned generation subsystems that are operated by other entities. Finally, this requirement could force the exchange of confidential information between entities. Standards CIP-003-4 and/or CIP-004-4 should take this into account when they are revised.
APPA	Disagree	We disagree with the need for BES Subsystem identification as discussed below under Question #6.
Consumers	Disagree	Changing classification will, in most cases, result because the transmission operator or reliability coordinator changed something. As such, this isn't likely to occur without the transmission operator or reliability coordinator knowing it first. This requirement needs to be for the Transmission Subsystem owner to notify the generator operator and generation owner when conditions change such as to make a generation subsystem potentially change categories. This identifies only one way communications from the generation provider to the transmission provider. It should be in both directions. In addition, Transmission Owners/Operators/Providers and Load-Serving Entities need to be exchanging information in a similar fashion. In addition, the current required shared information is not adequate. The critical function that the asset is providing needs to be shared. Also, at least the cyber system needs to be identified, but possibly details about such may also need to be shared.
NPCC	Agree	
MPPA	Disagree	MPPA supports the requirement to report the identification of High and Medium impact generation subsystems. However, as written, this requirement does not place the same burden on Transmission Owners to report their High and Medium impact systems.
Central Lincoln	Disagree	See answer to #4.
NERC	Agree	1. Ensure the language captures notification of all transmission elements in a Cranking Path for any identified blackstart generation resources. 2. In order to support compliance activities, add the following and update the Measures section appropriately: R2: add text to require the documentation identified to be signed and dated (by proper personnel identified per CIP-003 / R2). 3. Requirement R2 – change "developing" to "determining" in line 6.
Dominion	Disagree	Although Dominion agrees with most portions of R2, Dominion suggests the following modifications: "…..shall, within 30

Organization	Yes or No	Question 5 Comment (Response page 17)
		calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide written notification to the Primary Compliance Contact of the Transmission Owner or Distribution Provider to which the BES generation asset is directly interconnected ….” A Responsible Entity that owns any Generation Subsystem is prohibited, in many cases, from access to the data necessary to determine whether its facility could affect or influence the impact of BES Subsystems on the Bulk Electric System. Dominion believes, therefore, that in many cases, the Reliability Assurer, Transmission Planner or Resource Planner must make this determination and notify the Generator Owner of the results of their impact determination (e.g., high or low).
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	The purpose states that the Generators Owners categorization would not be proper unless the Transmission Owner has the Generator Owner’s security control information. This requirement is unnecessary and should be deleted as it is covered between R1 and R3.
Dyonyx	Agree	
MISO	Agree	
Westar	agree	
Green Country	Disagree	Why not change it from a bottom up approach to a TOP down request approach for the initial categorization. i.e. Transmission Operator requesting from GO/GOP. Then upon registered entity updating a system use a bottom up outlined here. It would make the flow of data and control of it a lot smoother.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	The first two clauses of the Requirement, “To support . . .” and “to ensure . . .,” are purpose statements that don’t seem to be appropriate to include in a requirement. Do these clauses include an obligation for TOs to classify their equipment that interfaces with a Generation Subsystem in the same way that the Generator Owner does? If so, this could cause a “race to the top” in which equipment rated by one Responsible Entity rates at a Medium BES Impact and rated by another Responsible Entity rates at a High BES Impact would have to be rated High by both entities. This would render the categories less meaningful.

Organization	Yes or No	Question 5 Comment (Response page 17)
PSEG	Disagree	Comment #1: This requirement seems to duplicate our understanding of the goal of Requirement 1 and therefore should be deleted. In order for an entity to meet the intent of Requirement 1 they need to understand both the BES Cyber System being reviewed and the elements that could be compromised through that BES Cyber System. In other words if a BES Cyber System can influence both a Transmission Substation device and a Generating Plant's device then both have to be considered as a single subsystem and identified as such for requirement 1. Example: A BES Cyber System if compromised allows access to both elements in a transmission substation and a generating plants production has to be identified per requirement 1 as a single subsystem. In addition to our concern that this standard is duplicative to requirement 1 we have a concern with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Example: Standards CIP-003 through 009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control. One specific concern is if someone was terminated with cause an entity has a limited amount of time to remove that person's access. Because this requirement is requiring the sharing of information an entity may not be able to secure the necessary commitments from different parties that termination information (this example) is communicated within X amount of time. Comment #2: This is an improvement on the current approach, however we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is High, should they notify the generation subsystem owner? For all future assessments as well? Further we are concerned in regards to a subsystem being classified differently and approved as such by two different RC's. Comment #3: Changing classification will, in most cases, result because the transmission operator or reliability coordinator changed something. As such, this isn't likely to occur without the transmission operator or reliability coordinator knowing it first. This requirement needs to be for the Transmission Subsystem owner to notify the generator operator and generation owner when conditions change such as to make a generation subsystem potentially change categories.
WE-Energies	Disagree	While Wisconsin Electric Power Company feels this approach of reviewing defined asset impact categorizations with connected transmission operators, the current requirement does not address areas around handling discrepancies of categorization between Transmission Operator and Generator Owner/Operator.

Organization	Yes or No	Question 5 Comment (Response page 17)
Idaho Power	Agree	
SOCO	Disagree	In the High and Medium categories, generation subsystems are allowed 30 days to submit information to the Transmission subsystem owners. We suggest that this same 30 day grace period be allowed in the Low category as well. Suggest that 2.1 be revised to read “and other identifiers which may assist in identifying the Facility(ies)”
DTE	Agree	
AEP	Disagree	Refer to question #2 above.
Edison Mission	Agree	
Calpine	Disagree	A regional authority would be the better responsible entity for this requirement.
NS&T	Agree	We agree with this proposal in principle, but we note that the proposed requirement does not specify what Transmission asset owners/operators must (or must not) do with the information they have been given. Would the Transmission asset owner/operator be compelled to change their subsystem categorization if the Generation asset owner/operator had designated their subsystems at a higher impact level? If so, could the Transmission asset owner/operator challenge this forced upgrade? Who would adjudicate such a challenge? We also wonder if this proposed requirement could create difficult non-disclosure issues in some cases. At the very least, the information that Generation asset owners/operators are directed to share would be considered "protected information" under the *current* Standards.
Flathead	Agree	This seems reasonable for High or Medium Impact facilities, but prefer annual requirements to lessen the paperwork burden.
E ON	Disagree	The requirement implies a Transmission Subsystem owner’s input into the categorization of unaffiliated Generation Subsystems. R1 already provides a Reliability Coordinator backstop role in reviewing and insuring proper categorization of BES Subsystems. E ON U.S. is also troubled by the statement: “. . . to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets.” The Transmission Subsystem owner alone should be responsible for identifying security controls for all owned transmission assets.
Carthage		CWEP has no comments for 5.
WECC	Agree	
Entergy	Disagree	This is an exercise in meaningless administration and inter-organizational coordination, with tangible unsavory regulatory

Organization	Yes or No	Question 5 Comment (Response page 17)
		consequences for failure which provide no practical benefit to anyone, much less reliability of the BES.
LCRA	Agree	
FRCC		In the main body of the requirement it states that the Generation Subsystem owner has to provide certain information to the Transmission Subsystem owners that are directly interconnected to them. This may seem to be a nit, but how will a Generation Subsystem owner know who has Transmission Subsystems? The compliance registry or functional model does not have a function for that and there are only TO's and TOP's registered. If the definitions are removed after consideration of previous comments, it may be something for the drafting team to think about in terms of other registered functions. In addition, the information that is required to be shared can be extremely confidential and there is no requirement for how this information will be maintained by those that receive it.
NIPSCO	Disagree	We believe this is an improvement on the current approach; however we are concerned with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Additionally, we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is high, should they notify the generation subsystem owner? Further we are concerned in regards to a subsystem being classified differently and approved as such by two different RA's / RC's. Suggestion: Clarify the responsibility of all entity types for information sharing and clarify the intended information protection requirements.
ConEd	Disagree	The Standard should stipulate an implementation requirement: the GO's categorization must be shared with the Regional Entity within 6 months of the Standard approval by FERC. The RE must in turn must share (within 30 days) the categorization with any impacted TO's.
O&R	Disagree	The Standard should stipulate an implementation requirement: the GO's categorization must be shared with the Regional Entity within 6 months of the Standard approval by FERC. The RE must in turn must share (within 30 days) the categorization with any impacted TO's.
Alliant	Agree	We believe the introductory statement : To support the . . . security controls for their assets," adds nothing to the requirement and should be deleted.
Ameren	Agree	
Black Hills	Agree	What happens in a jointly owned situation where the TOP receives two different assessments of impact? Which prevails?
TNMP	Disagree	TNMP supports the approach of requiring those with access to information to be responsible for providing it to other Entities that need the information. However, the 30 calendar day notice is not enough time to make a Transmission Subsystem CIP-compliant if its impact rating were upgraded (e.g. Low to Medium or Medium to High). If the Generation

Organization	Yes or No	Question 5 Comment (Response page 17)
		Subsystem change is planned, then the notification needs to be a point far earlier than 30 days from when the actual change occurs. Twelve calendar months should be standard to guarantee that CIP-compliance projects, which can incur significant costs, can be incorporated into annual fiscal budgets. An alternative would be for the Responsible Entity of the impacted Transmission Subsystem to have 12 calendar month once notified of a change to bring the Transmission Subsystem into compliance, as is provided for unplanned changes
NVEnergy	Disagree	We disagree for two reasons: First, the team should observe strong caution about the communication of Impact Categorization data. In the current version of CIP-003, there are strong controls specified around the protection of information related to Critical Assets and Critical Cyber Assets. In fact, even the lists of such Assets are themselves to be protected and cannot be revealed to individuals without a proper clearance via Personnel Risk Assessment and requisite Cyber Security Training. This Requirement as proposed seems to open a door to release of sensitive information worthy of high security protection to virtually unknown and un-verified parties, and would be a clear violation of the existing requirements related to Information Protection programs as specified in the existing CIP-003. Second, the 30-day period is overly burdensome on the industry. As well, it is not understood how a Transmission subsystem owner could be unaware of the characteristics of an interconnecting generation subsystem, which would necessitate such notification. As stated previously, the focus should be upon those cyber systems that can have measurable impact upon the reliability of the BES.
Empire	Disagree	I disagree with the 30 day requirement and would suggest that the 30 days be moved to allow 120 days. This will allow entities who require higher authority approvals enough time for proper notification.
SWTC	Disagree	Subsystems add an Unneeded Step and Adds Confusion: • Several have pointed out that we can get to the same classification analysis by either defining subsystems and then determining their impact on the BES, or starting directly with the worst case scenario analysis of a malicious use of a cyber system. Hence, some of us have questioned the purpose of adding the step of defining Subsystems to the analytical process, which seems unneeded. • In addition, since the draft does not define how groups of Facilities are to be grouped into cybersystems, than how do we know if the groupings themselves are correct and auditable. I can envision a situation where the auditors disagree with the entity on how Facilities are to be grouped into subsystems. Or would we get into the same situation where entities are allowed to define subsystems however they want and a potential for mistrust by regulators that we may have manipulated the definition of these subsystems in a way that causes us to avoid much of the CIP standards? • It may be simpler, more straightforward and less confusing to skip the step of defining subsystems and simply ask ourselves the question: What's the worst case scenario that can be caused by a malicious use of a cyber system? • This will cause us to have to inventory all of our cyber systems, but, I don't believe we were ever going to avoid that, even with defining subsystems.

Organization	Yes or No	Question 5 Comment (Response page 17)
SCEG	Agree	
Exelon	Disagree	In order to avoid possible confusion with Organizational registration we suggest that the SDT replace the “Transmission Subsystem owners”, with “owner of the Transmission Subsystem”. In addition we believe that the current wording in the CIP Information Protection requirements will need to be revised to allow for the sharing of information as stated in this requirement.
BPA Trans	Disagree	Recommended Changes With the addition of new requirement #1, existing R2 becomes R3. We believe that this requirement is too narrow in scope, that it should also be applicable to other Subsystem owners. We have edited the requirement based on this belief: Requirement 3 R3. The Responsible Entity that owns any BES Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Subsystem, provide the following information to those Subsystem owners directly interconnected to that Subsystem: (Violation Risk Factor: High) R3.1. Description of the Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies) R3.2. The Responsible Entity name R3.3. The BES impact categorization level Observation- There are potential situations where this type of communications requirement should also apply to Transmission and Control Center Owners, it is not just a Generation issue.
HQT	Agree	
Allegheny Energy	Disagree	Although this is an improvement on the current approach, we are not sure how the situation may be resolved where a GO categorizes a generation subsystem as “High” but the directly connected transmission subsystem owner does not categorize the generation subsystem as High. Also, if the converse were to happen, it is not clear if the transmission subsystem owner needs to notify the generation subsystem owner? Furthermore, we are concerned in regards to a subsystem being classified differently and approved as such by two different RC’s.
KCPL	Disagree	Requirement 2.3 implies the Registered Entity to establish an impact categorization level. It some cases it will not be possible for Generator Owners to know the impact their generator has even with appropriate criteria. Consider the example of an IPP with one 500 MW generator surrounded by a robust Balancing Area of transmission facilities and generating facilities. This may be a LOW or NO IMPACT reliability impact. Consider the same IPP in an isolated area starved for reactive voltage support. This could be a HIGH. The Transmission Operator or the Reliability Coordinator would be the appropriate entity to apply appropriate criteria and establish an impact level. The Standard needs some additional thought as to the process to consider when multiple facilities are brought together and the requirements to

Organization	Yes or No	Question 5 Comment (Response page 17)
		establish an appropriate categorization level.
Connectiv Energy	Agree	
MidAmerican	Disagree	Modify CIP-002-4 R2 to maintain the list of BES assets (instead of Critical Assets). BES bright line criteria also eliminate the need for proposed CIP-002-4 R2 that addresses directly interconnected facilities. All facilities are held to the same bar across the industry.
CPG	Disagree	GO/GOPs lean heavily on TO/TOPs in assessing their assets as the TO and the TOP have a wider system view of the BES than the GO/GOPs do. For example, a large generating facility may not be as critical to the BES as a smaller facility in a critical area. This Requirement should be reworded to ensure that the TO/TOP and GO/GOPs have an open dialogue as to how they categorize their assets and how they affect the assets directly connected to them.
Santee Cooper	Disagree	See comment for #4.
OGE	Disagree	The Transmission Subsystem Owner is dependent on the quality and timing of the Generation Subsystem Owner. There is risk that the Transmission Subsystem Owner and Generation Subsystem Owner may have differences in the impact categorization.
Oncor	Agree	We feel the introduction statement “To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets,” adds nothing to the requirement and could be deleted.
PPL Supply	Disagree	Agree with the need for Generation Owners to notify TOs of changes, but also there exists a need for reciprocal communication of Generation asset inclusion in system restoration plans or reliability must run status, and results from system reliability or stability analyses for which Generation asset owners have no data to perform independent analyses yet determine the asset’s impact on the reliability of the BES.
St. George	Agree	
NGRID	Disagree	Please clarify 2.2 – which Responsible Entity – GO or TO? Another concern is that Standards CIP-003 through CIP-009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control.
MGE	Disagree	This information is already provided within the following NERC Standards: FAC-001-0, FAC-002-0, FAC-009-1, PRC-001-1, PRC-015-0, TOP-005-1.1. Please clarify why the owner of the Generation Subsystem is required to notify the Transmission Subsystem owners directly interconnected to that Generation Subsystem and what the Transmission Substation owner is to do with the

Organization	Yes or No	Question 5 Comment (Response page 17)
		information once it receives it? This will also place an undue burden on the Transmission Subsystem owner when they initially determine that one of their subsystems may be Low BES Impact but the Generator Subsystem owner determine that their subsystem is Medium or High BES Impact. This will cause the Transmission Subsystem owner to elevate the impact of their facility to equal the Generator Subsystem category. Many companies are not vertically integrated and this cause serious non compliance issues. In order for R2 to have the maximum positive impact on assuring an adequate level of reliability, the Transmission Subsystem owner would also need to inform the Generator Subsystem owner the same information when a Transmission Subsystem is categorized as a High BES or Medium BES Impact for those Subsystems that are connected to each other.
FE	Disagree	R2 correctly requires a Transmission Subsystem owner to consider connected generation but improperly confines the consideration to Generation Subsystems. The problem with R2 is that it does not allow for the possibility that a substation which is part of a Transmission Subsystem may be serving a set of generators, that while not a Generation Subsystem in and of itself, is > 2000 MW or meets another BES Impact threshold. In such a case, the Transmission Subsystem should adopt a BES Impact that is a function of the generation characteristic as well as the transmission characteristic, i.e., the higher of them. In other words, the Transmission Subsystem owner must consider connected generation as a general matter, outside of the generators' potential Cyber System. Consequently, the Transmission Subsystem owner requires no notification by the generator – the Transmission Owner will already have general information about its connected generation. Therefore, R2 is not needed, and Attachment 1 should be modified to expand the scope of Transmission Subsystem thresholds to consider the size and scale of its connected generation. For example, Attachment 1 1.1 should require a High BES Impact for "Each Generation Subsystem or Transmission Subsystem exclusively connected to generation with aggregate rated name-plate generation of 2,000 MVA..."]
TECO	Agree	We believe that there should be direction within the standards as to how the Transmission Subsystem Owner should categorize its subsystems based upon the categorization of the generation subsystem.
CECD	Disagree	1. The phrase "to support the proper categorization of BES subsystems as identified in R1" should be deleted because the Purpose of the standard has already been stated. 2. If High and Medium category BES subsystem information is going to shared, notification requirements applying to parties of High or Medium status should apply to all Responsible Entities and not be limited to communication by a Generation Subsystem to a Transmission Subsystem owner.
MRO	Agree	We feel the introduction statement “To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets,” adds nothing to the requirement and should be deleted.

Organization	Yes or No	Question 5 Comment (Response page 17)
GTC	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2. We suggest changing "Transmission Subsystem owners" to "Transmission Subsystem owners and operators."
Xcel	Agree	
BGE	Agree	We support this notification proposal and approach as it encourages information sharing between generation and transmission owners. It would be beneficial to also add Transmission Operators as a party of this Requirement.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Consider removing this requirement. It is not clear why a Transmission Subsystem owner would need to have information on the ranking of Generators. In cases where the Generator is an independent entity from the Transmission Owner, revealing some of these information may result in a question of confidentiality. Generator Owners for the Generator Subsystem are generally not able to adequately perform an assessment of the impact of their Transmission Subsystem; the Transmission Providers themselves would be able to make this assessment much better as they have real-time operating data to perform such an analysis.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes this is an improvement over the current approach, however we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is High, should they notify the generation subsystem owner?
FMPA	Disagree	Again, Subsystem is an unnecessary and redundant step in the process. FMPA does not see a reliability need for this requirement and we recommend removing it. Transmission Owners / Operators and Generation Owner / Operators will be using the same criteria of Attachment 1, so, in what scenario will they arrive at a different answer for the same Subsystem?
Duke	Disagree	We disagree with the approach of categorizing BES Subsystems, but do agree that communication and coordination is required when entities make changes to Cyber Systems and security controls that could impact interconnected entities.
NBSO	Agree	
AESI	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to

Organization	Yes or No	Question 5 Comment (Response page 17)
		provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2. We suggest changing "Transmission Subsystem owners" to "Transmission Subsystem owners and operators."
IESO	Agree	
Manitoba 2	Agree	
OMPA	Disagree	OMPA agrees with the communication requirements; however, does not agree with the requirement to identify the BES subsystems.
ATC	Disagree	This requirement seems to duplicate our understanding of the goal of Requirement 1 and therefore should be deleted. In order for an entity to meet the intent of Requirement 1 they need to understand both the BES Cyber System being reviewed and the elements that could be compromised through that BES Cyber System. In other words if a BES Cyber System can influence both a Transmission Substation device and a Generating Plant's device then both have to be considered as a single subsystem and identified as such for requirement 1. Example: A BES Cyber System if compromised allows access to both elements in a transmission substation and a generating plants production has to be identified per requirement 1 as a single subsystem. In addition to our concern that this standard is duplicative to requirement 1 we have a concern with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Example: Standards CIP-003 through 009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control. One specific concern is if someone was terminated with cause an entity has a limited amount of time to remove that person's access. Because this requirement is requiring the sharing of information an entity may not be able to secure the necessary commitments from different parties that termination information (this example) is communicated within X amount of time.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their

Organization	Yes or No	Question 5 Comment (Response page 17)
		systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound

Organization	Yes or No	Question 5 Comment (Response page 17)
		engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
PSE	Agree	Puget Sound Energy agrees with the notification process. The aspect of a GO that is independent of the BA/TOP performing their own categorization still leaves the opportunity for inconsistent categorization across a system meaning all the Transmission Subsystem could be determined to be High and all the supporting Generation Subsystems to be Low. If the intention is to ensure reliability operation there needs to be a method of gaining consistency.
IMPA	Disagree	IMPA has concerns about the privacy and confidentiality of this important information to other entities and how this information will be kept or who will have access to it. This process needs to ensure that confidentiality agreements are in place with the recipients. If this information needs to be provided to the Transmission Subsystem owners, what entity will be responsible to ensure the entities who need to provide this information receive a listing of the appropriate Transmission Subsystem owner(s)? IMPA recommends that Generation Subsystem owners provide their information to the Reliability Coordinator who will be responsible for providing it to the appropriate Transmission Subsystem owner(s).
ERCOT	Disagree	ERCOT ISO recommends that the requirement be revised to make the required action more prominent in the wording of the requirement. Justification information is not necessary. "Each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem."
PacifiCorp	Disagree	Modify CIP-002-4 R2 to maintain the list of BES assets (instead of Critical Assets). BES bright line criteria would also eliminate the need for proposed CIP-002-4 R2 that addresses directly interconnected facilities.
NEI	Disagree	A) To avoid confusion with organizational registration, replace "Transmission Subsystem Owners" with "Owners of the Transmission Subsystem". B) R2 rightly requires a Transmission Subsystem owner to consider connected generation but improperly confines the consideration to Generation Subsystems. The problem with R2 is that it does not allow for the possibility that a substation which is part of a Transmission Subsystem may be serving a set of generators, that while not a Generation Subsystem in and of itself, exceeds 2000 MW or meets another BES Impact threshold. In such a case, the Transmission Subsystem should adopt a BES Impact that is a function of the generation characteristic as well as the transmission characteristic, i.e., the higher of them. In other words, the Transmission Subsystem owner must consider connected generation as a general matter, outside of the generators' potential Cyber System. Consequently, the Transmission Subsystem owner requires no notification by the generator – the Transmission Owner will already have general information about its connected generation. Therefore, R2 is not needed, and Attachment 1 should be modified to expand the scope of Transmission Subsystem thresholds to consider the size

Organization	Yes or No	Question 5 Comment (Response page 17)
		and scale of its connected generation. For example, Attachment 1 1.1 should require a High BES Impact for "Each Generation Subsystem or Transmission Subsystem exclusively connected to generation with aggregate rated name-plate generation of 2,000 MVA …"] C) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Organization	Yes or No	Question 6 Comment (Response page 18)
Progress Energy	Disagree	We believe Attachment 2 goes beyond what should be the scope of the CIP standards and the focus needs to be on real-time cyber operations. In addition, CIP-003 through -009 Version 4 needs to be defined before we can agree to this requirement.
Dynegy	Agree	
GSOC/OPC	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with the BES Cyber System itself. We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will far outweigh its benefits. It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
Hayden	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
SDGE	Agree	
APPA	Disagree	APPA Task Force Comments: CIP-002 – Attachment 2: Functions Critical to the Reliable Operation of the Bulk Electric System The APPA Task Force recommends that the SDT either eliminate Attachment 2 or convert it to a reference/guidance document supporting the standard. The important criteria of the standard are included in Attachment 1. The conceptual discussion of functions in Attachment 2 only adds redundancy, complexity and confusion. If Attachment 2 identifies "functions critical to the reliable operation of the Bulk Electric System," there should be a one-to-one mapping of these functions to each of NERC's other reliability standards. Also, how are these functions different from those described in the Functional Model? Is Attachment 2 essentially another, different, functional model? At best, Attachment 2 should be treated as a list of "things to consider" when developing worst case scenarios/contingencies for evaluating the impacts of "unavailability, degradation or compromise" of a Cyber System. If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? Unless Attachment 2 is treated as a guidance document, the identification of reliability functions cannot be open-ended, implying that additional functions, or aspects of functions, have yet to be identified. The SDT should avoid open-ended statements such as: "Aspects of the Managing of Constraints include, but are not limited to" that are followed by a bulleted list. Further, the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. From this perspective, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is certainly NOT critical. Calculation of ACE is certainly NOT critical since ACE values are double-checked with neighboring BAs on separate Cyber Systems, ensuring identification and correction of errors. This standard should focus on what is truly critical: threats of an Adverse Reliability Impact resulting in "instability, uncontrolled separation, or cascading" outage. If Attachment 2 is retained, APPA suggests that it should be renamed: "Activities Performed to Maintain the Reliable Operation of the Bulk Electric System."
Consumers	Disagree	This needs to be based on the cyber systems that are at risk. The definition of BES Cyber System is not appropriate. If "BES Cyber System" is replaced with "critical cyber assets", then this would be appropriate. But that would lead us back to where we are now, so there is no need to change the existing standard. As we have noted earlier, this "inheriting" of the same BES impact from the subsystem is flawed. In such a scenario, a printer would inherit the same category as a server. This is the same issue that was identified as a problem in the earlier versions of CIP-002 that the SDT seemed to be trying to move away from. Each RE should categorize and list those cyber assets associated with a High Impact subsystem (as recommended, medium and low terminology not used) but not list those with no impact. For those listed, a second evaluation of the cyber assets should then be performed and

Organization	Yes or No	Question 6 Comment (Response page 18)
		recorded, eventually in the cyber asset list.
NPCC	Agree	
MPPA	Agree	
Central Lincoln	Agree	Central Lincoln agrees with this in general, but please consider the APPA Task Force comments regarding attachment 2.
NERC	Agree	1. In order to support compliance activities, add the following and update the Measures section appropriately: R3: add text to require that the documentation created when categorizing and subsequent documentation called for in R3.1 & R3.2 to be signed and dated (by proper personnel identified per CIP-003 / R2). 2. Requirement R3.2 – add the word "level following "same BES impact" in the first sentence.
Dominion	Disagree	The function performed by the cyber system as well as the criticality of the BES Subsystem should be examined to identify the criticality of a BES Cyber System.
Encari	Disagree	As earlier commented we feel that Attachment 2 can be strengthened to include additional components - the actual requirements above we do agree with.
US ACE – NW	Agree	
SCE	Disagree	A cyber system supporting a BES subsystem may not always warrant the same impact level as suggested by Requirement 3.2. Factors such as: (a) the role of the BES cyber system within the broader context of the operation of the BES subsystem (Is this the only mode of failure of the BES subsystem?); (b) the technical capabilities of the cyber system (Does it provide information sensing capability or interactive control?): (c) the nature of the network that the interconnected BES cyber system is using (IP or serial); and (d) the connectivity if any outside a BES sub-system (Is remote access allowed?); are examples of the factors to consider. Impact level determination can be a combination of the function (as listed in Attachment 2), the impact level of the BES subsystem, and the degree to which it is interconnected. The interconnectedness of a cyber system is a significant contributor to its security vulnerabilities.
USBR	Disagree	It is sufficient that the BES systems are assessed to have an impact. The degree of an impact is superfluous.
Dyonyx	Agree	
MISO	Agree	
Westar	Agree	agree with the concept of the highest impact level being assigned. I do think that Attachment 2 just adds confusion and should be eliminated.
Green Country	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
Oregon PUC		No comment
NB Power Gen	Disagree	3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that [is connected bi-directionally (routable protocol, modem) outside of the perimeter of the electronic security perimeter contained within the facility it is installed in and, if accessible remotely] has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.
Manitoba 1	Agree	
Portland GE	Disagree	Requirement 3.2 could spur a “race to the top” in which everything connected to a High BES Impact system would have to be rated High as well. This could provide incentives to Responsible Entities to keep their systems disconnected because connecting them would bring them all under the scope of a higher level of controls. For example, Section 3.2 uses the term “associated.” However, everything could be interpreted as “associated” and may “affect” the Subsystem. The SDT should recognize that even though a Cyber System may affect or be associated with a BES Subsystem, it could have little impact on the BES, regardless of the Subsystem’s impact on the BES.
PSEG	Disagree	Comment #1: We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problem from CIP Version 1). Comment #2: We believe that this needs to be based on the cyber systems that are at risk. The definition of BES Cyber System is not appropriate. If “BES Cyber System” is replaced with “critical cyber assets”, then this would be appropriate. But that would lead us back to where we are now, so there is no need to change the existing standard. Suggestion: 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI’s comments regarding this question. In addition, Wisconsin Electric Power Company feels there is potential for confusion in R3.1, because some systems touch so many other BES “subsystems”.
Idaho Power	Disagree	Cyber systems may have varying levels of impact on the functionality of the BES Subsystem and therefore, may not need

Organization	Yes or No	Question 6 Comment (Response page 18)
		the same level of protection. To categorize every cyber system at the same level as the BES subsystem adds an unnecessary burden on the registered entities.
SOCO	Disagree	This is a bit troubling that all the pieces have to take on the criticality of the highest impact level of the parts. The listing of the Cyber System should be based on a top down approach rather than a bottom up approach. Only after a BES Subsystem is classified as a High or Medium Impact, should the Cyber System related to it should be classified as High, Medium Impact. This will provide a more functional approach that will provide the same result while being less resource intensive. The control system for a Generation Unit may be classified as a High Impact, but classification of a pH monitor or ambient air sensor connected to the control system, not essential for generation operation should not required to be classification at the High classification. Suggest wording – Each Responsible Entity shall list each BES Cyber System which is critical to the operation of the BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any Functions Critical to the Reliable Operation of the Bulk Electric System. Delete entire paragraph - “For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems.”
DTE	Agree	
AEP	Disagree	Refer to question #2 above. The SDT took a good start in Appendix 2 of segmenting the standard into a functional approach. However, we believe that this section is not yet fully developed and should be comprehensively reviewed by SMEs to determine and describe, on a bright line basis, what is specifically in scope and out of scope for each of the functional areas. While helpful in better defining the functional areas, the use of the exhaustive list of descriptions leads to interpretation issues of what is meant to be included and not included by the descriptions, and will not get to the bright lines that are sought to define what specifically needs to addressed.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	As I read this multiple medium impacts equal a high, does not make sense. Either it has one high or not.

Organization	Yes or No	Question 6 Comment (Response page 18)
E ON	Disagree	E ON U.S. does not agree with assigning each cyber system the same level of criticality as the most impactful subsystem. Some cyber systems associated with a generating station, for example, do not impact the BES if disabled (e.g., emissions monitoring systems).
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	The size/rating of a "BES Subsystem" (whatever that is – say, for sake of discussion, a substation) has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. A 69kV substation with a routable network link to its control host data center presents much higher adverse cyber security risk than an EHV substation served only by legacy serial communication lines to its control host. Pick any "BES Subsystem" and this fact remains the same.
CenterPoint	Disagree	Disagree – See comments to 1.a. It is unclear what the SDT hopes to accomplish with this requirement when compared to the existing requirements under CIP-002, especially when this proposal has been unveiled in a piecemeal fashion. If the SDT's intent is to extend a set of cyber security requirements to non-critical cyber assets, the SDT could propose such a set without the contortions and flaws of this proposed new classification system. Moreover, it may not be appropriate for a BES Cyber System to automatically inherit the impact of the associated BES Subsystem because the cyber system may not be essential to the operation of the associated BES system, a concept correctly captured by the existing CIP-002 standard. Furthermore, if the SDT were to leave the definition of cyber systems as proposed in this draft, cyber security risk would also have to be considered in determining the impact level of the cyber system. For example, a Cyber System that does not use a routable or dial-up connection to communicate externally should be categorized as low impact because it is not vulnerable to remote attacks, regardless of the impact of its associated BES Subsystem.
LCRA	Agree	
NIPSCO	Disagree	We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problems from CIP Version 1). Suggestion: Eliminate the BES protection level inheritance. Allow the cyber assets to be evaluated based on the impact to the asset, not based on the impact of the asset to the BES. If this inheritance approach is left as proposed by the SDT, we would need to see how the one size fits all approach is being addressed throughout CIP-003-4 through CIP-009-4.
ConEd	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
EEI	Disagree	EEI believes that it is appropriate to evaluate cyber assets based upon accessibility and span of control. Therefore facilities such as Control Centers would be expected to contain multiple cyber assets that would be designated as high impact cyber assets. However, the cyber assets that are operated or managed from a Control Center would not necessarily be designated as high impact cyber assets, unless: 1. They have the ability to control other cyber assets or, 2. if, when destroyed, degraded or otherwise rendered unavailable: they could directly cause, contribute to, or create an unacceptable risk of- - BES instability; and/or - BES separation; and/or - a cascading sequence of failures. Or in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of- - instability; and/or - separation; and/or - a cascading sequence of failures; Or could hinder restoration to a normal condition. The current definition: "The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time." Is inappropriately overbroad, by including planning horizon. EEI suggests that the definition be modified to focus on time sensitive – real-time operations, e.g. "The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in real-time." In addition, elements of BES Cyber systems maintenance, such as change management are important, but should not necessarily be protected in the same manner as real-time systems operations.
O&R	Agree	
Alliant	Agree	See Question 12 for specific comments on Attachment 2 criteria.
Ameren	Disagree	The impact levels of high, medium and low associated with the BES Cyber Systems should also be evaluated with the high, medium and low impact level of their associated BES Subsystem and appropriate controls developed for the different combinations of categorizations of BES Subsystem & BES Cyber System as in the following matrix.

Organization	Yes or No	Question 6 Comment (Response page 18)
		BES Subsystem BES H/H M/H L/H Cyber H/M M/M L/M System H/L M/L L/L The effort to develop these nine different response levels initially would of course be higher up front but the granularity gained in this approach would allow for a more focused and efficient application of protection controls for the BES Cyber Systems identified.
Black Hills	Agree	
TNMP	Agree	TNMP agrees with the concept of assigning the highest impact level of the associated BES Subsystem to the BES Cyber System. However, the lack of clarity on the definitions of Cyber System and BES Cyber System mentioned earlier makes it difficult to determine exactly what the highest impact level would be applied to. Additional guidance, through definitions or other means, is needed to provide clarity or “bright lines” and improve this requirement. It may be necessary to create a requirement before this one or another criteria attachment giving guidance on how one goes about determine what makes up a BES Cyber System if the definition alone does not provide adequate clarity.
NVEnergy	Disagree	It is more appropriate to evaluate cyber assets based upon accessibility and span of control than by simply assigning the impact degree of the highest impact BES subsystem. For example, control centers are undoubtedly some of the highest impact BES subsystems under consideration; however, not all of the cyber systems within the control center carry that same level of impact. Hence, as suggested in comments above, the impact of the cyber systems themselves should be assessed first, then whether they are associated with a High Impact BES subsystem. Equally important, we urge the drafting team to acknowledge that the CIP security objectives should target only those cyber systems that are accessible via connections such as routable protocol, IP, and dial-up. Self-contained cyber systems, no matter their degree of importance, are not subject to the type of threat that the CIP standards have set out to address. Certain physical protections may be appropriate in these instances.
MWDSC	Disagree	See prior comments on lack of clarity in definitions and need for a "No BES Impact" category.
Empire	Disagree	I do not agree with assigning each cyber system the same level of criticality as the most impactful subsystem. Some cyber systems associated with a generating station, for example, do not impact the BES if disabled.
SWTC	Agree	If a common element roughly spans several facilities does this force all elements of those facilities to be high even if singularly they are low or medium. The way the standard is written it requires them to be high.
SCEG	Agree	
Exelon	Disagree	While we agree with the need to appropriately categorize and document BES Cyber Systems, we ask the SDT to consider including provisions for exceptions as well (e.g. non-routable protocol, lack of dial-up capability). As stated

Organization	Yes or No	Question 6 Comment (Response page 18)
		previously, Exelon is hoping for a timely and clearly stated scope of applicability from NERC and the NRC to U.S. nuclear plant generator owners/operators in order to provide a clear "bright line" to provide the needed guidance for implementation
BPA Trans	Disagree	1. This approach does not take into consideration how much the Cyber System can affect the Subsystem. A Cyber System whose loss, degradation, or compromise has only a minimal effect on a BES Subsystem could have very little impact on the BES, regardless of the Subsystem's impact on the BES. BOTH the impact of the Cyber System on the Subsystem, as well as the impact of the Subsystem on the BES, must be taken into account. 2. Using the methodology in the Standard could result in applying overly-stringent standards to Cyber Systems. To use a print server as an example, a Control Center print server supporting hardcopy reports could be construed as supporting Control & Operation as well as Situational Awareness. The lack of hardcopy reports could be construed to be an adverse effect on the Control Center. If the Control Center is of High impact on the BES, then so would be the print server. Yet, if the hardcopy is a last-ditch backup to online displays, the actual impact on the BES would be very small. Assigning a High BES impact to the print server would be inaccurate. A much better choice would be to determine the impact of the Cyber System on the Subsystem, in some manner that must be defined. In most cases, one could then limit the BES impact of the Cyber System to be no higher than its impact on the BES Subsystem it supports. With the addition of new requirement #1, the existing R3 becomes a new R4. Our changes to R4 are too extensive to be represented as edits to existing R3. Therefore, new R4 is rewritten in its entirety: R4. The Responsible Entity shall categorize and document BES Cyber Systems as follows: (Violation Risk Factor: High) R4.1. The Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R2, that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. R4.2. The Responsible Entity shall assign the BES impact categorization to each listed BES Cyber System which represents its potential impact on the BES Subsystem it supports. Where a BES Cyber System is associated with more than one BES Subsystem, the responsible entity shall assign the BES impact categorization level to that BES Cyber System that represents its highest potential impact to any of the associated BES Subsystems. The concept of greater and lesser security boundaries are not necessarily applicable in many utility situations. With this in mind, it is our opinion that the potential adverse impact of a cyber system on a BES Subsystem may not necessarily be significant enough that it would degrade the Subsystem(s) it supports, or the Bulk Electric System, enough to justify an impact of the level that matches that of the Subsystem itself. Cyber Systems should be graded on their own potential impacts on the subsystem(s) and the BES rather than simply being assigned the impact rating of the Subsystem(s) to them.
HQT	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
Allegheny Energy	Disagree	We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problem from CIP Version 1).
KCPL	Agree	With appropriate definitions and criteria for Attachments 1 and 2, these concepts should work.
Connectiv Energy	Disagree	Accomplishing 3.1 implies that an entity identify ALL cyber systems associated with each BES Subsystem and determine for each if it "has the potential to adversely impact any of the functions…". This is unnecessary for BES Cyber Systems that are associated with only LOW IMPACT BES Subsystems. Suggest modifying section 3.1 with a prefix similar to "For each BES Subsystem categorized as HIGH or MEDIUM impact, "
MidAmerican	Disagree	Change CIP-002-2 R3 to refer to the list of BES facilities (instead of Critical Assets). Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a “system.” Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls. Categorization level determinations should be addressed in the security control standards.
CPG	Disagree	Designating a cyber system impact solely on the impact of the BES subsystem is not a valid methodology in that it does not take into account the cyber system’s importance to the BES Subsystem. The current proposal may require an unimportant cyber system to be heavily protected for unnecessary reasons. Furthermore, R3.1 will require a listing of all cyber systems. This is not a worthwhile endeavor considering that many cyber systems are Low or No Impact for GO/GOPs. Listing only those cyber systems associated with High and Medium Impact subsystems is a far superior approach.
Santee Cooper	Disagree	While SC agrees that “one size fits all” is an incorrect approach to a standard, it seems as FERC is overtaxing the utilities to unnecessarily protect items that have no impact. Certainly, some assets have an impact to the utility and could cause inconvenience or local outages, but as a whole, if classified as FERC would like, would cause higher costs and higher rates for our customers.
OGE	Disagree	• In 3.1, the act of putting the Cyber System on the list makes it a BES Cyber System. Change this from BES Cyber System to Cyber System. • Every asset is High, Medium, or Low. There should be the option of some Subsystems being excluded, even from the Low Impact category. • We need some guidance for identifying the appropriate set of cyber assets. There seems to be no way to

Organization	Yes or No	Question 6 Comment (Response page 18)
		develop a "practical" list that makes sense without assessing the risk of all cyber assets.
Oncor	Disagree	The rationale for assigning of cyber security controls to BES Cyber Systems should recognize the real cyber threat of the cyber system to the reliability of the BES. The installation of a DFR in an EHV station does not necessarily have a “High BES Impact” and may not warrant “high” cyber security controls. We would support multiple levels (i.e., Low, Medium, High) to correspond with the appropriate level of cyber security controls and countermeasures appropriate for each cyber system.
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Disagree	The reference framework of electric grid engineering, facilities ratings, etc listed in Attachment 1 is not required and the alternative method sans the Attachment 1 criteria will be a better approach since the issues at hand needs to be approached from a networked-computing systems security engineering perspective. Hence, BES Impact Criteria in Attachment 1 should not be tied into.
MGE	Disagree	R3, “As a step in assigning appropriate security controls for its assets” should be deleted; the statement does not add content or instruction to the requirement. R3.1, Please clarify that only High and Medium BES Impact items are to be used in Attachment 2, since items listed in the Low BES Impact category do not have the potential to adversely affect the BES. R3.2, In order for R3.2 to have the maximum positive impact on assuring an adequate level of reliability, the Transmission Subsystem owner would also need to inform the Generator Subsystem owner the same information when a Transmission Subsystem is categorized as a High BES or Medium BES Impact for those Subsystems that are connected to each other.
FE	Disagree	FE believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
TECO	Disagree	Please see our comments to question 2. As currently worded, this requirement introduces a one size fits all approach to any cyber system associated with a BES subsystem at a particular level. Cyber Systems that have a direct impact on BES subsystems, such as those with operational and control capabilities, should be assigned a higher impact and protected at a higher level than those that have an indirect impact, such as planning systems, change control, etc.. Consideration must be given to the criticality of the BES cyber system and its impact on the reliable operation of the associated BES subsystem. Not all BES cyber systems associated with a high impact BES subsystem should be subject to the same level of requirements. For example a planning system such as a load forecast system should not require the same level of security as a control and operation system such as a SCADA. Systems without direct impact should either

Organization	Yes or No	Question 6 Comment (Response page 18)
		be given a lower impact level or be removed from consideration as BES Cyber Systems. This requirement should have a sub requirement that gives a time length for updating the Cyber System list after an update to the BES Subsystems list in R1.1 (or the addition or removal of a Cyber System independent of an associated BES Subsystem). As the requirement states now, the Compliance Enforcement Authority could expect an update to the Cyber System list to be made simultaneous to the BES Subsystem list, which is not practical. Sub-Requirement 3.1: In categorizing each BES Cyber System based on Attachment 2, a number of systems may be included that may be significant from an operational stand-point but have very low probability in terms of actual threats. Versions 1-3 of CIP-002 filter Cyber Systems by use of “routable protocols.” Given the current state of potential threats in terms of cyber security, there are no measurable threats to proprietary architectures not using routable protocols. We should continue to use the routable protocol filter as a measure of probability in the risk analysis required in Requirement 3. It is not supported that a plant DCS controller communicating on a vendor specific proprietary protocols is as High Risk as one that communicates through TCP/IP. While both are operational significant, the actual threat probability is much lower for the proprietary system. It is not clear how cyber systems such as firewalls, network infrastructure, physical security controls, and environmental controls will be assigned a BES impact level.
CECD	Agree	1. The phrase "as a step in assigning appropriate security controls for its assets" should be deleted because the purpose of the standard has been stated. 2. Agreement is based on the registered entity having flexibility to define its BES Subsystems and the ability to appropriately identify the impact to the BES.
MRO	Disagree	We feel the introduction statement “As a step in assigning appropriate security controls for its assets,” adds nothing to the requirement and should be deleted. Otherwise, we agree with the method in principle, however, see answers to questions 12 for specific comments on Attachment 2 criteria.
GTC	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with the BES Cyber System itself. We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will far outweigh its benefits. It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
Xcel	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
BGE	Disagree	Regarding BES cyber asset categorization, we feel that cyber assets should be evaluated based upon accessibility and span of control of the cyber asset. Under the current approach facilities such as Control Centers would have multiple cyber assets designated as high impact cyber assets regardless of the asset's true potential to impact the BES. The cyber assets that are operated or managed from a Control Center should not be designated as high impact cyber assets, unless: 1. They have the ability to control other cyber assets or, 2. if, when lost, degraded or otherwise rendered unavailable: they could directly cause, contribute to, or create an clearly defined unacceptable risk of: - BES instability; and/or - BES separation; and/or - a cascading sequence of failures. Or in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of: - instability; and/or - separation; and/or - a cascading sequence of failures; Or could hinder restoration to a normal condition.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	It appears that the revised standard does not provide a distinction between cyber systems that use a routable technology and those that are either completely isolated or connected through non-routable means (proprietary networks or layer 2 communication networks). Isolated Cyber systems should be considered a low risk and CIP-005 & 007 should not apply. In categorizing each BES Cyber System based on Attachment 2, a number of systems may be included that are significant from an operational stand-point but have very low probability in terms of actual threats. Versions 1-3 of CIP-002 filter Cyber Systems by use of "routable protocols."
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP agrees with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problems from CIP Version 1).

Organization	Yes or No	Question 6 Comment (Response page 18)
FMPA	Disagree	FMPA recommends that the SDT either eliminate Attachment 2 or convert it to a reference/guidance document supporting the standard. The important criteria of the standard are included in Attachment 1. The conceptual discussion of functions in Attachment 2 only adds redundancy, complexity and confusion. If Attachment 2 identifies "functions critical to the reliable operation of the Bulk Electric System," there should be a one-to-one mapping of these functions to each of NERC's other reliability standards. Also, how are these functions different from those described in the Functional Model? Is Attachment 2 essentially another, different, functional model? At best, Attachment 2 should be treated as a list of "things to consider" when developing worst case scenarios/contingencies for evaluating the impacts of "unavailability, degradation or compromise" of a Cyber System. If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? Unless Attachment 2 is treated as a guidance document, the identification of reliability functions cannot be open-ended, implying that additional functions, or aspects of functions, have yet to be identified. The SDT should avoid open-ended statements such as: "Aspects of the Managing of Constraints include, but are not limited to" that are followed by a bulleted list. Further, the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. From this perspective, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is certainly NOT critical. Calculation of ACE is certainly NOT critical. This standard should focus on what is truly critical: threats of an Adverse Reliability Impact resulting in "instability, uncontrolled separation, or cascading" outage. If Attachment 2 is retained, FMPA suggests that it should be renamed: "Activities Performed to Maintain the Reliable Operation of the Bulk Electric System."
Duke	Disagree	We disagree, and prefer the "Cyber First" approach whereby Cyber Systems are first identified that can impact functions essential to BES reliability. Next, these Cyber Systems should be categorized based upon their risk and impact to the BES. For example, a system may represent LOW risk to its associated BES Subsystem facility, but could pose HIGH risk to BES reliability if it is attached to a routable protocol control system network.
NBSO	Agree	
AESI	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with the BES Cyber System itself. We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will

Organization	Yes or No	Question 6 Comment (Response page 18)
		far outweigh its benefits. It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
IESO	Agree	
Manitoba 2	Disagree	All the devices or components in a BES Cyber System should not automatically inherit the categorization of the overall BES Subsystem. If many devices or components are part of the BES Cyber System, such as a plant control system, then the assessed impact could be Minimal (very low) for an individual device, such as a transducer. Redundancy (often mandatory requirements in other reliability standards) should be considered as it may reduce the impact of an individual BES Cyber System component. Redundant systems with different architecture or modes may require a lesser degree of security controls due to an inherent robustness, determined through a vulnerability assessment. Master ends of BES Cyber Systems may be categorized higher than the individual remote ends of the BES Cyber Systems, but no higher than the associated BES Subsystem.
ATC	Disagree	3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 6 Comment (Response page 18)</th></tr>
<tr><td></td><td></td><td>security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>R3.2 causes concern as it potentially overly burdens Low impact cyber systems by association because of the concept of defaulting to the highest BES impact categorization level assigned. Smart Grid could bring more cyber systems into scope in the future and this requirement could have significant implications resulting in entities having to treat many Cyber Systems as if they have higher impact than they do simply by association with something else.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA does not object to the requirement of assigning the highest impact level of the associated BES Subsystems, but we do have issues with Attachment 2.</td></tr>
</table>

Organization	Yes or No	Question 6 Comment (Response page 18)
		Attachment 2 has issues in itself such as the definitions used to define functions critical to the reliable operation of the BES. For example under number six (Control and Operation), the definition includes activities such as actions and conditions that provide monitoring and control of BES elements. Elements should be deleted and replaced with BES Subsystems. An element may be a 138 kV potential transformer that's used for local indication only. In addition an example aspect of Control and Operation is "All methods of operating breakers and switches (such as SCADA). What about manual operations?? Is the intent of this Standard to include any and all aspects of operating equipment?? If so then any station that has SCADA and has any equipment that can be operated either manually or remotely would have to be included and appropriate security controls applied. Attachment 2 also attempts to define "Situational Awareness" (number 8.) This is not a defined NERC Glossary Term so it needs to be defined. One of the aspects listed for the situational awareness function is "monitoring and alerting (such as EMS alarms)". This aspect would include every RTU installed in a BES facility. For example, Utility A may be interconnected at facility that is a High BES Impact facility. Utility A does not own, operate, or maintain the facility and their RTU may be used for "status only". But since the facility is High BES Impact then appropriate security controls would need to be put in place by Utility A for their RTU, even though the RTU is used for "status only". This could also apply to local indication, such a substation annunciator panel. Item 9 "Inter-Entity Coordination and Communication" could include all forms of communications such as voice, fax, and electronic (e-mail, text, etc.). This could potentially require the use of secure fax machines, secure voice lines, and encrypted electronic communications by smaller utilities when they communicate with a large Control Center that is determined to be a High BES Impact asset.
ERCOT	Agree	ERCOT ISO recommends that additional asset categories be addressed as well (i.e.: PSP, ESP, non-critical cyber assets, access control, monitoring, etc.)
PacifiCorp	Disagree	Change CIP-002-2 R3 to refer to the list of BES facilities (instead of Critical Assets). Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls. Categorization level determinations should be addressed in the security control standards.
PEPCO	Disagree	We believe that it is appropriate to evaluate cyber assets based upon accessibility and span of control. Therefore facilities such as Control Centers would be expected to contain multiple cyber assets that would be designated as high impact cyber assets. Please reference previous discussions.
NEI	Disagree	A) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's

Organization	Yes or No	Question 6 Comment (Response page 18)
		August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent “Cyber System Risk” and the horizontal access represent “BES Subsystem Impact”; that a none category be added both vertically and horizontally with the resulting categorization being “none”; that High-Low and Low-High results in “Medium”; and that Medium-Low and Low-Medium results in a “Low.” The resulting table outlines a graduated level for applying cyber security controls to BES Cyber Systems based on risk. BES Cyber Systems that have a low risk should not require the same cyber security controls as BES Cyber Systems that pose a high risk. Ratcheting the risk level to protect nearly everything will inadvertently result in a decline in the reliability of the BES. B) The size/rating of a “BES Subsystem” has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. A 69kV substation with a routable network link to its control host data center presents much higher adverse cyber security risk than an EHV substation served only by legacy serial communication lines to its control host. Pick any BES Subsystem and this fact remains the same. C) Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine “critical functional classifications”. We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Summary Consideration for VRF:

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
Progress Energy	Disagree	We don't believe that every subsystem should be categorized; only Facilities with High impact to the BES should have subsystems categorized. As new Facilities are added they would be evaluated and subsystems categorized if deemed a High impact Facility.
GSOC/OPC	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
SDGE	Agree	
APPA	Disagree	APPA Task Force Comments: The APPA Task Force believes that categorization of BES systems and subsystems are an administrative process and do not present a high risk to the BES. Therefore it should have a low VRF; however, improper application of security controls might increase the risk to the BES.
Consumers	Disagree	There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
NPCC	Agree	
SWPA	Disagree	
MPPA	Agree	
Central Lincoln	Disagree	Categorization does not equate to risk. The protection of the cyber equipment is what really matters, and might be sufficient regardless of whether they were categorized correctly or not categorized at all. Suggest Low for all requirements.
Dominion		Dominion could not locate the proposed VRFs in the review materials.
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
USBR	Agree	
Dyonyx	Disagree	Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Westar	Disagree	Should all be low.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE		No comment at this time
PSEG	Disagree	
WE-Energies	Disagree	Wisconsin Electric Power Company believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
Idaho Power	Agree	
SOCO	Disagree	
DTE	Agree	
AEP	Disagree	The requirements must be made much clearer in order to make the assessment of the appropriate level of VRFs.
Edison Mission	Disagree	Comments: Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	There should be lower or no VRFs related to Low Impact assets.
E ON	Disagree	
Carthage		No comments
WECC	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
Entergy	Disagree	If the fundamental logic of the process is faulty from the very beginning (starting with R1 & R2 coupled with Attachment I) then any subsequent discussion of VRF/VSL validity is moot.
LCRA	Agree	
NIPSCO	Agree	Did not review proposed VRF's
ConEd		The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
EEI	Disagree	EEI believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
O&R	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
Ameren	Disagree	We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
Black Hills		Not thoroughly reviewed at this time.
TNMP	Agree	
NVEnergy	Disagree	A Medium VRF is more appropriate for the three proposed requirements. Failing to execute any of the three requirements does not in and of itself pose any risk to the BES. However, the accompanying security control standards, if violated, would pose a higher risk more suited for a High VRF assignment.
Empire	Disagree	
SWTC	Agree	
SCEG	Disagree	Did not find the VRF’s in this document.
Exelon	Disagree	Exelon believes that the proposed Violation Risk Factors and Violation Severity Levels are overly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as the reference for version 4.
BPA Trans	Agree	
HQT	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
Allegheny Energy	Agree	
KCPL	Agree	It is reasonable for the assignment of a HIGH VRF for applying appropriate criteria in the categorization of facilities and cyber systems within those facilities applying appropriate criteria.
MidAmerican	Agree	VRFs: The violation risk factor for R1 changed from medium to high while the VRFs for R2 and R3 stayed at high. MidAmerican supports these risk factors for the changes to CIP-002-2 proposed by MidAmerican as long as the criteria are clear.
CPG	Disagree	There need to be VRFs for TOs and RCs not providing information to GOPs as required in Attachment #1, Sections 1.1, 1.2, 1.3, 1.4, 1.6, 1.13, 2.1, and 2.5. Furthermore, it is hard to assess Violation Risk Factors when the draft versions of CIP-003 through CIP-009 have yet to be developed. A broader system view of how all of these standards are intertwined is needed.
Santee Cooper	Disagree	
OGE	Agree	
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Agree	
MGE		N/A
FE	Agree	We generally agree, with exceptions as stated above for R1.
TECO	Disagree	
CECD	Agree	
MRO		We'll withhold comments on these sections until the standard is more set.
GTC	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
Xcel		We'll withhold comments on these sections until the standard is more set.
BGE	Agree	No comments
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
FPL	Disagree	Since each entity will have different risk assessments we recommend that additional input from industry be provided when determining the VRFs.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes that moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.
FMPA		FMPA has many disagreement with the details of the requirements, therefore, we believe it is premature to comment on VRFs and VSLs.
Duke	Disagree	Requirements and associated VRFs need to be revised to the “Cyber First” approach.
NBSO		No comment
AESI	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
IESO	Agree	
Manitoba 2	Agree	
IMPA		IMPA has no comments.
ERCOT	Agree	
PacifiCorp	Disagree	VRFs: The violation risk factor for R1 changed from medium to high while the VRFs for R2 and R3 stayed at high. PacifiCorp supports these risk factors for the changes to CIP-002-2 proposed by PacifiCorp as long as the criteria are clear.
PEPCO		We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
NEI	Disagree	The VRFs wer not locatable on NERC site nor in CIP 002-4 as posted.

Summary Consideration for VSL:

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
Progress Energy	Disagree	We believe documentation required for compliance is unnecessarily burdensome and would not improve the reliability of the BES.
GSOC/OPC	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
SDGE	Agree	
Consumers	Disagree	It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty.
NPCC	Agree	
SWPA	Disagree	
MPPA	Disagree	R#1 Moderate VSL should specify 31 to 60 days, and high VSL should specify 61 to 90 days, and Severe VSL should specify greater than 90 days to remain consistent with R#2.
Central Lincoln	Disagree	Paradoxically, un-categorized BES subsystems or cyber systems must be categorized prior to VSL determination. Once they are categorized, the violation has been fully mitigated. If the regional entity is performing this assessment anyway, perhaps they should be responsible for all categorization under CIP-002 to avoid duplication of work.
NERC	Disagree	1. R2 – make the timeframes consistent with the expectations in R1. 30-40, 41-50, 51-60. We require the Responsible Entity to update the list in these timeframes but do not require the Generator Subsystem owner to report the change in like timeframes. 2. R3 – the VSLs have gaps. For example in the Lower level, there is no violation if 1-4 BES Cyber Systems have not been categorized. There needs to be full coverage for all violations of the requirement to be consistent with NERC and FERC obligations. The other levels have similar issues. A remedy could be to assign impact levels based on the

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		number of BES Cyber Systems not categorized (1 for Lower, 2 for Moderate, 3 for High, More than 3 for Severe)
Dominion	Disagree	Dominion disagrees with the VSL level determinations due to the ambiguity associated with the high, medium and low categories. No compliance violation should exist if an entity categorizes its assets in good faith and has supporting documentation for such categorization. Dominion suggests removing such criteria from the VSLs.
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	How will the number of "true" categorization or number of subsystems be determined as the basis of measuring what missed or miscategorized? This severity level determination is far too reliant on an external judgment. The measurement needs to be absolute an unambiguous.
Dyonyx	Disagree	Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Westar	Disagree	Severity levels should be adjusted to reflect the actual potential impact to the BES which in most cases will be low.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE		No comment at this time
PSEG	Disagree	Comment #1: It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty. Comment #2: There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
WE-Energies	Disagree	Wisconsin Electric Power Company believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		as a pattern for version 4.
Idaho Power	Agree	
SOCO	Disagree	
DTE	Disagree	We disagree with the severe VSL for R1. Failure to update documentation should not carry the same weight as not categorizing any BES Subsystems. Moderate VSL for R3 should reference BES Cyber Systems, not BES Subsystems.
AEP	Disagree	The requirements must be made much clearer in order to make the assessment of the appropriate level of VSLs.
Edison Mission	Disagree	Comments: Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Calpine	Disagree	Severity levels for R1 non compliance: Failure to update the categorization list should be changed to 30 to 60, 60 to 90 and greater then 90 days for moderate, high and Severe respectively. Low impact BES subsystems have no effect on the BES and should not be in the violation security levels. Remove R1. Lower VSL and R3 Lower VSL criteria. Further to comments made under question 5 on this comment form... The responsible entity should inform the regional entity under the deadlines specified. The regional entity will inform interconnected subsystem owners... R3 server VSL should drop firs criteria related to responsible entity it appears to be redundant. The severe violation should only entail ignoring the standard requirements.
NS&T	Agree	
Flathead	Disagree	
E ON	Disagree	Severe violation for failing to update BES categorization within 50 days after a change (R1.1) is too high. With respect to R3, if a non-affiliated BES subsystem owner fails to correctly categorize its BES subsystem leading the Transmission Subsystem owner to assign too low a categorization to its cyber systems, then it may lead the Transmission Subsystem owner to incorrectly categorize its associated cyber system. Assigning a severe VSL to the Transmission Subsystem owner under these circumstances is inequitable.
Carthage		No comments
WECC	Agree	
Entergy	Disagree	If the fundamental logic of the process is faulty from the very beginning (starting with R1 & R2 coupled with Attachment I) then any subsequent discussion of VRF/VSL validity is moot.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
CenterPoint		It is difficult to judge the VSLs because, as illustrated in our comments to question 8, it is difficult to define what the "subsystem" should be or how many "subsystems" exist.
LCRA	Agree	
NIPSCO	Disagree	It seems unreasonable to move from a Moderate - High - Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty. Suggestion: Review the VSL / VRF details and remove the double time penalty option. Additionally, review the penalty equity between an entity who mis-categorized a BES subsystem and an entity who has not categorized any.
ConEd	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard. Failure to update the categorized list for a decommissioning of a BES subsystem being categorized and a high severity does not make sense. There is no exposure to any threats, so why would this be high severity?
EEI	Disagree	Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented, program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
O&R	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
Ameren	Disagree	We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
Black Hills		Not thoroughly reviewed at this time.
TNMP	Agree	
NVEnergy	Disagree	We disagree with the VSL's, particularly with regard to the high severity determination for the instance of missing or mis-categorizing only one BES subsystem. Given the degree of subjective judgment that is involved with the categorization, it seems inappropriate to assess such a severe violation level for what could amount to a disagreement between the Entity and the Auditor on the Impact of a particular BES subsystem. Perhaps the VSL's should be based upon the completion or failure to complete a categorization exercise itself.
Empire	Disagree	Severe violation for failing to update BES categorization after a change (R1.1) is too high. These are administrative in nature and provide no impact to the BES therefore they should be a low VSL.
SWTC	Agree	
SCEG	Agree	
Exelon	Disagree	Exelon believes that the proposed Violation Risk Factors and Violation Severity Levels are overly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as the reference for version 4.
BPA Trans	Disagree	For R1, the VSL refers repeatedly to not categorizing a BES Subsystem of some impact level. Yet, without the categorization having taken place, how can the impact level have been determined? Also, the VSL refers to miscategorized Subsystems. Who determines that the Subsystem was miscategorized? Will the Regional Entities be performing their own independent categorization? R2. No comment. R3. This has the same issues as R1. How does an entity know the Impact level of a Subsystem that has not been categorized? Who makes the determination?
HQT	Agree	
Allegheny Energy	Disagree	It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has miscategorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty.
KCPL	Disagree	The VSL's for Requirement 2 are based on the Registered Entity with generation to know their categorization level, which they may not be able to assess as explained in the response to question 5, so I think the VSL will need some additional

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		work. In general, I struggle with the inclusion of the LOW in the VSL for Requirement 3 as if the reliability impact is LOW, what is the point of a penalty considering the NERC concerns are preserving the highest levels of reliability impact.
MidAmerican	Disagree	VSLs: Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented; program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120); and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented; high-controls not implemented; moderate-reviews not completed; lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
CPG	Disagree	As written, a Responsible Entity will receive an increased VSL based on a time period, and then a higher penalty due to the length of time a violation existed. A severity level change should not be based on time, but rather another quantifiable measure. As for the VSLs for Requirement #3, a percentage of subsystems based on the entities cumulative total subsystems should be used instead of number of subsystems. That way, an entity with a lot of subsystems would be judged as fairly as an entity with a much smaller amount. Furthermore, it is hard to assess Violation Severity Levels when the draft versions of CIP-003 through CIP-009 have yet to be developed. A broader system view of how all of these standards are intertwined is needed.
Santee Cooper	Disagree	Every utility is different, with different impacts on their neighbors and the BES. The same mistake at a small utility would not have the same impact of a much larger utility.
OGE	Disagree	Miscategorized BES elements as a Severe VSL should not be warranted based any residual risk that might be present due to inadequate control sets.
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Agree	
MGE		N/A
TECO	Disagree	We support EEI's comments regarding proposed Violation Risk Factors and Violation Severity Levels. In addition, we offer the following suggestions for improvement. For R1, Lower VSL: By definition, Low Impact BES Subsystems have no impact on the BES, therefore they should not be listed under Violation Severity Levels. We suggest "One to three Medium Impact BES Subsystems have not been

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		categorized or have been miscategorized as Low Impact." Then updating Moderate VSL to "Three or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact." For R3, Lower VSL: By definition, Low Impact BES Subsystems have no impact on the BES, therefore they should not be listed under Violation Severity Levels. We suggest "One to three Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact." For R3, Moderate VSL: Add "Cyber" after "BES." Per the current R3 VSLs miscategorizing 1 or 2 Medium Impact BES Cyber Subsystems will NOT result in a violation. The suggested change to R3, Lower VSL above will solve this issue. For R3, Severe VSL: The last sentence states "The Responsible Entity does not have a list of ALL its BES Cyber Systems." Technically this means if the entity misses listing even one of its Low Impact BES Cyber Systems they would have committed a severe violation. Suggest changing "all" to "any."
CECD	Disagree	It appears excessive that 1 improper categorization of an asset is considered High, as does applying a Severe VSL for more than 1. Utilizing numeric values to change the VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems.
MRO		We'll withhold comments on these sections until the standard is more set.
GTC	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
Xcel		We'll withhold comments on these sections until the standard is more set.
BGE	Disagree	It appears excessive that miscategorizing an asset (see R1 under High and Severe VSLs) is considered "High" for 1 miscategorization and "Severe" for more than 1. Utilizing numeric values to change VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems, that is: should an entity that has a 1000 subsystems be penalized the same as an entity that has 10 subsystems when both miscatagorize 2 subsystems. Additionally, we feel that increasing the VSL every 10 days for a failure to update does not justify a change in severity level.
Springfield, MO		No comment at this time
FPL	Disagree	We disagree mainly b/c of the inclusion of low impact BES subsystems, as stated earlier.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes that moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.
FMPA		FMPA has many disagreement with the details of the requirements, therefore, we believe it is premature to comment on VRFs and VSLs.
Duke	Disagree	Requirements and associated VSLs need to be revised to the “Cyber First” approach.
NBSO		No comment
AESI	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
IESO	Agree	
Manitoba 2	Disagree	The Violation Severity Levels appear inconsistent by equating a missed deadline for updating the categorized BES Subsystem list, with not categorizing any BES Subsystems under the Severe Violation Severity Level. All the deadlines for the VSLs should be 30 days, with differences based on impact level categorization. R1 Lower VSL should include “The Responsible Entity has failed to update its categorized list of Low BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the Moderate VSL should be changed to “The Responsible Entity has failed to update its categorized list of Medium BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the High VSL should be changed to “The Responsible Entity has failed to update its categorized list of High BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the R1 Severe VSL should be removed. The quantity thresholds used in the Violation Severity Level table should be a weighted score of an entity’s subsystems, where multiple Low BES Impact Subsystems or BES Cyber Systems are considered equivalent to single High Impact BES Subsystem or BES Cyber System, respectively.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
IMPA		IMPA has no comments.
ERCOT	Agree	
PacifiCorp	Disagree	VSLs: Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented, program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
PEPCO	Disagree	Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points.
NEI	Disagree	A) The requirements must be made much clearer in order to make the assessment of the appropriate level of VSLs. B) It is unfair to assess a penalty on categorization errors, given the vagueness of the terminology as noted elsewhere in the response.

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria?

Summary Consideration:

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
Progress Energy	Need to have CIP003 through -009 Version 4 defined before we can respond appropriately. We request that CIP003 through -009 Version 4 be provided for review prior to the formal comment period.
Dynegy	1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a “Must Run” unit to add the following phrase at the end of the sentence: ”that have wide area reliability impacts.” 3. Add an Item in Category 2 that corresponds to Item 1.3 for “Must run” units that have “local area reliability impacts.” 4. In Item 2.6., the word “controlling” needs to be clarified. This item should only encompass Control Centers and back up Control Centers that “remotely control and solely monitor the status of assets” rather than just performing redundant monitoring of those assets.
GSOC/OPC	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
Hayden	As stated earlier in question 1.h the definition for "Medium Impact" is too vague and needs to be more specific to help the analyst figure out what the difference is between High and Medium impact and how to assign the impact level.
SDGE	• Define vague terms – For example, what is unacceptable risk, what is a “normal condition”, what does “directly affect the electrical state” mean? In order for the CIP Standards to be interpreted and applied equally across the industry, these terms need to be defined specifically or changed so that there is no ambiguity. • As mentioned above, we are advocating having two impact choices (High BES impact and No BES impact). We feel this makes more sense as we start to think about the other CIP Standards and the various requirements. We don’t want to have “high impact” and “medium impact” portions of the various requirements, as that would be too confusing to keep straight and implement successfully. • We feel that by including the “planning time frame criteria” in the “High Impact” and “Medium Impact” definitions, it adds a level of

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	great deal of complexity to the process without a corresponding benefit to the reliability of the BES. • In the event that the SDT keeps the "planning time frame criteria" in the definitions, please define information such as study load levels, assumptions for line overloads (100% of applicable ratings, for example) to determine if cascading outages are possible. This is to ensure all parties are viewing reliability using the same consistent set of criteria. Further clarify cascading outages (we feel that loss of minimal load such as less than 100 MW should be low in impact). • If the drafting team declines to eliminate one of the high, medium, or low impact classifications, the drafting team should consider more operational definitions of high, medium, and low BES impact.
APPA	APPA Task Force Comments: Attachment 1 Criteria for BES Impact Categorization of BES Subsystems: High BES Impact (H): The APPA Task Force recommends that criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region). Bright line thresholds (such as 2000 MVA or 2000 MW) are useful default values that should be used in the absence of a particular BES design value used in a region for planning studies and real-time operations. The EPAct, FPA Section 215(a)(4) defines "reliable operations" as: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements," so, to boil it down, the EPAct passed into law mandatory standards to regulate the industry in its efforts to avoid "instability, uncontrolled separation, or cascading failures" This definition of "reliable operation" is nearly synonymous with the NERC Glossary term for "Adverse Reliability Impact": "(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." "Cascading" is further defined by the NERC Glossary as: "The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies." The focus of the standard ought to use this concept of Adverse Reliability Impact to define what is High risk, Medium risk and Low risk. Supply/Demand Mismatch and IROL: Starting from this theoretical basis, what kinds of conditions can cause an Adverse Reliability Impact, such as widespread frequency related instability? The answer really is a large mismatch of supply and demand (even faults can cause instability by "shorting out" the load, causing a large mismatch of supply and demand) or operating conditions, regardless of cause, that lead to violation of an Interconnection Reliability Operating Limit (IROL). Therefore, the entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs. The rest of Attachment 1 is simply a restatement of conditions that can cause these metrics to be exceeded. IROL is defined in the NERC glossary as: "(a) System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Cascading Outages that adversely impact the reliability of the Bulk Electric System." IROLs are determined by study by the PAs and TOPs and these metrics are readily available in accordance with FAC-014. Hence, the only metric that remains to be established is the supply/demand mismatch. This mismatch can be caused in a few ways: 1. Tripping a large amount of generation through malicious use of cyber systems 2. Tripping a large amount of load due to malicious use of cyber systems to directly trip the load (e.g., use of a large SCADA system to activate a centralized UFLS system). 3. Tripping key transmission Facilities by malicious use of cyber systems that could cause voltage instability, thermal cascading, etc., that could in turn result in a large mismatch of supply and demand, the large mismatch of supply and demand being the key. (For example, the Northeast Blackout of 1965 was caused by loss of tie lines importing power from Canada causing a large supply/demand mismatch, and the Blackout of 2003 was caused first by thermal cascading, which in turn caused a voltage collapse of Cleveland and Detroit, which then resulted in a huge supply /demand imbalance through the loss of two major urban centers) The APPA Task Force recommends that the SDT develop a metric for supply/demand mismatch (e.g., the Contingency Reserves of the region, or another metric determined by study) that correlate with High and Medium Impact. High Impact should include those events that have a relatively high chance of causing an Adverse Reliability Impact, e.g., cause an IROL to be exceeded or a supply / demand mismatch greater than a certain metric. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC. 1000 MVA may be an acceptable default value in the absence of a specific regional threshold based on the largest single contingency for a PC or RC. Blackstart and Cranking Paths: If a cascade were to occur, utilities need to be assured that their blackstart units and cranking paths to other generators that are identified in the regional restoration plan will be available, and that the control systems for these devices have not been compromised. The Task Force understands the need for protection of the “critical units” and “critical paths,” but the identification of all blackstart units as High Impact is not reasonable or necessary to ensure BES restoration. APPA Task Force discussions indicate that that some of the Regional restoration plans were developed with different and inconsistent methodologies. There have been reports that some regions have just rolled up into their restoration plans all blackstart-capable units identified in each utility’s local restoration plan. This in effect designates all blackstart units as high impact in regions that are using this as a practice. The APPA Task Force recommends that the categorization of blackstart units and transmission cranking paths between the blackstart units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, “High Impact” from a restoration perspective should focus on preventing restoration efforts and “Medium Impact” should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent blackstart efforts from multiple blackstart units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder blackstart efforts from a single blackstart

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	unit or cranking path in the regional plan. Blackstart capable units that are not in the regional plan should be Low Impact. Recommendation of Edited Language to High BES Impact (H): 1. High BES Impact (H) 1.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the Contingency Reserve or total Reserve Sharing Obligations of a Reserve Sharing Group or, if no Contingency Reserve or total Reserve Sharing Obligation has been established, a supply loss of 2000 MVA or a load loss of 2000 MW. 1.2. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.3. A BES Cyber System, that if maliciously used, can result in exceeding one or more Interconnection Reliability Operating Limits (IROL's). 1.4. A BES Cyber System, that if maliciously used, can prevent blackstart restoration efforts from multiple black start units and cranking paths identified in the regional restoration plan. The APPA Task Force believes using the above criteria would make Attachment 1 very simple, resulting in only four criteria instead of the 16 in the "High Impact" list proposed by the SDT. Most of the 16 items in the "High Impact" list are simply phenomena that can cause supply/demand mismatch greater than the established metric, or an IROL to be exceeded (e.g., voltage collapse, thermal cascading, loss of situational awareness, etc.) We recommend including these phenomena as subsections of the four criteria spelled out above. We believe such a method is much simpler to understand and enforce, and is more in line with what ought to be regulated - phenomena that can cause an Adverse Reliability Impact. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC. Recommendation of Edited Language to Medium BES Impact (M): Medium Risk should be those events that would put the system dangerously close to an additional contingency causing an Adverse Reliability Impact, e.g., an event that could cause a supply / demand mismatch greater than the largest loss of source that would put the system in a status whereby a single contingency could cause a supply / demand mismatch greater than the Contingency Reserves of a reserve sharing group, or an IROL to be exceeded, (at a point only a single contingency away). Also, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 1000 MVA may be an acceptable default value for the Medium BES Impact threshold in the absence of a specific regional threshold based on the largest single source contingency. 2. Medium BES Impact (M) 2.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the single largest loss of source contingency of the region, or, if no single largest loss of source value has been established, a supply loss of 1000 MVA or a load loss of 1000 MW. 2.2. A BES Cyber System, that if maliciously used, can result in a system state whereby the next single contingency would cause the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	BES to exceed an IROL. 2.3. A BES Cyber System, that if maliciously used, can hinder regional blackstart restoration efforts by preventing blackstart from a single black start unit and cranking path identified in the regional restoration plan. Low BES Impact (L): Low Impact should include all other BES Cyber Systems that have a low risk of contributing to an Adverse Reliability Impact. The APPA Task Force cautions the SDT that even though the Low BES Impact category will have the least Adverse Reliability Impact, it will have the most burdensome and widespread impact on registered entities for compliance purposes. We cannot stress this point enough; the industry needs assurance that the Low BES Impact requirements will be reasonable. This category must be aligned with the cyber system protections that are programmatic in nature and are not cyber system specific. These requirements should be similar to the current CIP-002, which require a risk based assessment methodology where entities can manage compliance through employee training on the security of cyber assets, implementation of policies for the creation and protection of passwords, implementation of policies for access, etc. Making the compliance requirements exceedingly strict will take valuable resources away from the protection of the high and medium impact assets. The industry's first priority should be to protect and secure the high and medium impact facilities.
Consumers	Comment #1: Resolve the confusion of terms used in the proposed glossary additions. Comment #2: Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities' obligation. Comment #3: Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the aggregate load shedding capability or to the single step load shedding increment. Comment #4: There seems to be inconsistency in the use of MW vs. MVA Comment #5: We believe that the standard shouldn't use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement mod-024 Comment #6: We would like to understand the engineering basis for selection of MW criteria Comment #7: The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Comment #8: Nowhere in this proposed standard is it identified the benefit of the classification levels. Unless there are different security requirements specified for the different classifications, this is a meaningless exercise.
NPCC	Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. The detailed Attachment 1 definition does give clarification. In any system where the Contingency Reserve is less than 2000 MW, clause 1.2 dominates clause 1.1 so engineering evaluation cannot be used to reclassify a Generation Subsystem into having a Medium BES Impact.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. Request clarification on the wording "leaving" in 1.5. Alternatively, suggest 1.5 be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station… Request clarification where 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include the distribution facilities necessary to complete the cranking path (facilities necessary to restore generation)? If 1.10, 1.11 and 1.12 should be removed and language added to 1.7 as follows: Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) (or SOLs for those areas that do not identify IROLs), or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method. Request clarification on 1.13, which SPS 300 kV threshold (550 kV or higher for the Quebec Interconnection), sensing, action, or both? A SPS has a sensing portion and a portion that takes action. Sometimes these are not the same voltage, same station, etc. Also, 1.13 should be made to read: Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact. Request clarification on "automatic load shedding" in 1.14. If this refers to underfrequency load shedding then Distribution Provider must be added to the Applicability Section. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center". Request clarification on wording "leaving" in 2.2. Alternatively, suggest 2.2 be made to read: Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, 300 kV or higher for the Quebec Interconnection, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines connected to the station… Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add ", including as notified by the Generation Owner". Consistent with 1.9, recommend changing 2.4 from "NUC-001-1" to "NUC-001". Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? A SPS has a sensing portion, and a portion that takes action. Sometimes these are not the same voltage, same station, etc. Alternatively, suggest 2.5 be made to read: Each Protection System, Special Protection System (SPS), or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, less than 550 kV for the Quebec Interconnection, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. Consistent with the comment on 1.15 and 1.16, recommend changing from "Control Center and backup Control Centers" to "Primary Control Center and any backup Control Centers" in 2.6.
SWPA	Section 2.5: This section should include a lower voltage limit of 100kV for protection systems.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
MPPA	The criteria for High, Medium and Low BES Impact should also be referenced by the definitions to maintain consistency. MPPA recognizes and concurs with the need for a multi-tiered approach.
Central Lincoln	1.1 There is no requirement for any of these entities to approve/disapprove assessments. 1.3 Pre-designated by who? 1.4 See 1.1 1.7 A huge burden. Simulations must be run for every individual bus and every individual line out of service? 1.8 This statement makes no sense. Including what? 1.10 See 1.7. 1.11 See 1.7. 1.12 See 1.7 2.1 See 1.1 2.2 See 1.1 2.3 See 1.1 3 See answer to 1.i. above. Please also see the APPA Task Force's suggestions on simplifying Attachment 2
TransAlta	Under High BES Impact section, item 1.2 states, "Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations". In the NERC "Security Guideline for the Electricity Sector: Identifying Critical Assets" approved by CIPC on Sept. 17, 2009, Page10, Table C-2, has the wordings for essential generation for the BPS (BES), specifically for the contingency reserve consideration. These two wordings are different. It is suggested that the draft team clarify item 1.2. Besides, the contingency reserve requirement in NERC BAL-002 standard applies to BA's, and the contingency reserve number may not be accessible by the generator owners/operators. As this criterion is written inside the draft standard right now, it will unduly put extra requirements for the generator owners/operators to get the contingency reserve from BA's . If the draft team want to keep it as a "bright lines" approach, then there should be some requirements in the standard which stipulate such data sharing among the different registered entities when performing the BES impact categorization.
NERC	1. Attachment 1 is overly complex and violates the intended outcome of "straightforward and objective". As stated previously, there is concern whether the Reliability Assurer or Reliability Coordinator has the available resources or desire to adjudicate Responsible Entity impact classifications and this would drive to eliminate this aspect of the criteria. 2. Part 1.2 – more specificity is required with regard to the timeframe of interest to identify the largest contingency reserve obligation. 3. Part 1.4 – reword to state "Each Blackstart Resource that has been included in a Transmission Operator's restoration plan per EOP-005. 4. Part 1.6 – reword to state "Each Transmission Subsystem that includes a Cranking Path used in a Transmission Operator's

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	restoration plan per EOP-005. 5. Parts 1.10 – through 1.12 should be combined into one criterion for separation, cascading outages, etc. There is no meaningful distinction in separating the cause (e.g. frequency, voltage, or other collapse). 6. Part 1.13 – This criterion should be separated into two: one for Protection Systems for which the voltage distinctions would apply, and second for SPS and RAS for which the voltage distinction has no meaning. 7. Parts 1.13 and 2.5 – Eliminate Part 2.5 entirely. If the impact to the BES is the same, there can be no meaningful distinction between High and Medium. Therefore, modify 1.13 to remove the voltage classes, and remove the "Adverse Reliability Impact" reference and make consistent with the language used in Parts 1.10 – 1.12. 8. Part 1.16 – criterion should be separated into two: one for Balancing Authorities and one for Transmission Operators. For the Balancing Authority criterion, the language could read: "Each Control Center and backup Control Center performing Balancing Authority functions for load and generator exceeding 2000 MWs. For the Transmission Authority part, there is little relevance to the 2000 MW threshold. Therefore, it should be rooted in the transmission line delineations outlined in earlier criteria as follows: "Each Control Center and backup Control Center performing Transmission Operator functions for switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 kV or higher in other Interconnections, with three or more non-radial transmission lines leaving the station" 9. Medium Impact – modify the Protection System description in R2.5 with the less than 300 kV East and West, and less than 200 kV thresholds for others; modify the Balancing Authority and Transmission Operator control center criteria to use the 1000 MW threshold and similar voltage thresholds consistent with R2.2, respectively.
Dominion	Dominion suggests the following modification to the high category: High BES Impact (H) 1.2. Any Critical generating unit or plant whose aggregate output exceeds the value of the Contingency Reserve Requirement.
Encari	See comments made regarding definitions.
SCE	A "Not Applicable" or "No Impact" category should be added to the criteria.
USBR	It is not clear that the criteria proposed is necessary or consistent with the impacts described in the standard. 1.1. What was the basis for 2,000 MVA? Is it likely for the GO to perform the study that this refers to, or is it more likely to be by the TOP, Balancing Authority, Reliability Coordinator or the Reliability Assurer? None of whom are required to cooperate in such a study. 1.2. This requires the GO to have knowledge that the BA/TOP is not required to share. 1.3. What are these "Reliability "must run" units"? These are not defined, so it leaves a question on what is meant, is this a marketing term that does not belong here? Is it referring to a Generator that must run for system reliability, whose loss or failure to operate will result in an Adverse Reliability Impact? 1.4. If there is not a Cranking Path defined to which the black start Generation Subsystem interconnects, it should not be required to have a high BES impact.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1.6. With no requirement to talk to your neighbor, the TOP could determine a Cranking Path which passes through one of our yards, and should be flagged as part of such, but we would have no knowledge thereof. This ties back to /R2, which says neighbor TO's should also have to communicated High Medium with each other… 1.8. As there are no bilateral communications required the GO would not be aware of this situation. In addition, the phrase "including as notified by the Generation Owner" appears to be a back reference to the very standard which refers to this Attachment. 1.13. As currently worded, all SPS/RAS/PS would be exempt as none of these systems are operated at kilo-Volt level. They may protect systems that operate at that level. What are Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem? These are not defined.
Dyonyx	Attachment # 1 has many issues, a number of which have been presented in the paragraphs below according to their numbered paragraphs: 1.1 The arbitrary 2,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why "name plate MVA" rating has been designated versus "net output" based parameters. 1.3 Reliability "must run" units are frequently old units to be retired but held in an operational mode for MW capacity or VAR capabilities. Some regions are disbanding these unit designations. Accordingly, we do not believe that all "must run" designated units should categorically be included as High impact. 2.1 The arbitrary 1,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why "name plate MVA" rating has been designated versus "net output" based parameters. Lastly, we are not of the opinion that an interruption of this arbitrary value of generation necessarily will "directly affect the electrical state …..of the BES." For example, EROCT has a Contingency Reserve of 2,300 MW. The term "capability" of the BES is not an appropriate provision, e.g., the loss of even 10 MW will impact the total "Capability" of the regional system, but this is not the intent of the standard.
FMPP	Item 1.16 refers to CC performing BA or TO functions for transmission assets or generation assets of 2000 MW or more. What this sentence says is any CC with TO functions for transmission assets is High BES Impact. Transmission assets is lower case in this sentence so it is not defined. This sentence should be broken into two sentences one for BA and one for TO. How much transmission assets triggers a high impact should not use MWs, should use miles of 200kV and over or BES related or something related to TO. Item 2.6 does not refer to BA or TO. What this sentence says is any CC controlling transmission assets is Medium BES Impact. Again transmission assets is lower case so is not defined; also this sentence should be broken into two sentence one for BA and one for TO functions.
MISO	1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a "Must Run" unit to add the following phrase at the end of the sentence: "that have wide area reliability impacts." 3. Add an Item in Category 2 that corresponds to Item 1.3 for "Must run" units that have "local area reliability impacts."

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	4. In Item 2.6., the word “controlling” needs to be clarified. This item should only encompass Control Centers and back up Control Centers that “remotely control and solely monitor the status of assets” rather than just performing redundant monitoring of those assets.
Westar	Use the NERC defined term of Adverse Reliability Impact to categorize High Impact BES elements. Should replace the Low Impact Category with No Impact. The lack of routable protocol or dial up access should still be a consideration in the categorization level.
Green Country	I still would like to see a "No BES" Impact category.... exempt from CIP-003 thru CIP-009
Oregon PUC	Again, we recommend that the Low BES Impact level be eliminated.
Manitoba 1	Communication should be clarified, difference between dial up and LAN and the extent of the firewall. It is possible for banks to maintain firewalls so i think the level of the firewall would make a difference.
Wolverine	I agree conceptually with the categorization of assets into high, medium, and low BES impact. My concern is that what needs to accompany this draft in order for all to properly evaluate it, is a definition or proposal of what types and degrees of security controls would accompany each category of asset. For example: Currently, if an entity determined through their RBAM that they have "no critical assets", then none of the controls and requirements of CIP-003 through -009 apply. Under this new proposal, let's assume the same entity would declare all assets to be "low impact". What type and level of security controls then apply to these "low" impact assets? None? (As per the old system?) Without information on the level of controls associated with this categorizing scheme, it is difficult to fully evaluate this concept.
Portland GE	No comment at this time
PSEG	Comment #1: Resolve the confusion of terms used in the proposed glossary additions. Comment #2: Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities’ obligation. Comment #3: Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the aggregate load shedding capability or to the single step load shedding increment. Comment #4: There seems to be inconsistency in the use of MW vs. MVA Comment #5: We believe that the standard shouldn’t use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement mod-024 Comment #6: We would like to understand the engineering basis for selection of MW criteria Comment #7: The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Comment #8: Nowhere in this proposed standard is it identified the benefit of the classification levels. Unless there are different security requirements specified for the different classifications, this is a meaningless exercise.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
WE-Energies	High BES Impact: • 1.2 a generator does not itself have a Contingency Reserve obligation or a RSG, MISO determines this and may vary as facilities may be out of service and the obligation may reduce. Moving target. • 1.3 needs to better define Reliability "must run", formal contract, reliability "out of market" dispatch (run our peaking generating stations for reliability now and again) could be moving target, or have Market implications. • 1.7 to include anything that a TLR would be called for is not High, should be Low if anything. • It's not clear under what conditions 1.7, 1.8, 1.10, 1.11 and 1.12 apply. We could create scenarios where the events described could occur, but would not reflect normal operating conditions we expect. This relates back to the inclusion of the "planning time frame" comments made earlier. For how many contingencies do we assess the impact?
Idaho Power	Attachment 1 of the proposed CIP-002-4 appears to focus on typical criteria that would be part of a system planning study. These studies generally are based on N-1 and N-2 criteria which address only the loss of an asset(s), not the manipulation of the asset(s) thereby missing the point of Michael Assante's letter dated April 7. 2009 that states; "system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word "manipulate" here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new "cyber security" paradigm."
SOCO	In 1.1, the Regional Reliability Assurer is only defined in the Functional Model version 4, which is not approved yet. Also, NERC has issued a SAR to modify the NERC Glossary of Terms (issued 1-22-10 and comments due on 2-22-10) and this new Assurer is not shown in this modification either. We suggest just allowing the Reliability Coordinator for your region or subregion to be the approver. In 1.3, it describes listing "pre-designated as Reliability must run" units as a High Impact. In many large systems, this list of must run units changes on a daily basis, often for maintenance work in the area or even voltage support at various times. Since this would require an update every day, we suggest making only the "permanently assigned" units be on this list. A general note about the use of engineering analysis. It should be recognized by the drafting team and NERC staff that some conditions cannot be discovered without the use of an engineering analysis. For example, in 1.7, IROL's and TLR's are found by using studies in either the Planning time frame or the Operating time frame. Similarly, in 1.10, 1.11 and 1.12, voltage collapse, frequency related instability and cascading outages are all typically recognized in either the Planning time frame or the Operating time frame using engineering analysis. Therefore, in 1.1and 1.5, the drafting team and NERC staff should recognize that the same engineering analysis should be deemed credible when excluding generation and transmission subsystems that do not have an impact on the BES reliability when they are outaged. In 1.4, some very large systems have many blackstart units with multiple paths to multiple units it can start up. This makes no sense to protect them all and could be a waste of resources. Attachment 1, section 1.5 – Recommend that this definition be removed entirely or moved to the Medium Impact section; loss of individual Transmission Subsystems simply because it is above a specific voltage level does not cause BES instability, separation, or cascading failures.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	In 1.6, when discussing cranking paths, we suggest that 1.6 be moved to be next after 1.4, when discussing blackstart generation, if indeed the intent is to relate blackstart units to the cranking paths to some designated generation. Attachment 1, section 1.6 – a large utility with multiple blackstart units has multiple options for Cranking Paths; recommend that this definition be moved to the Low Impact section. In 1.7, by the definition of subsystems at the beginning of the document, this would potentially place ALL substations and generating plants in the High Impact category regardless of the system configuration. There are certainly those assets that this would be true for, but the majority of the time, we can do without almost ANY element. Attachment 1, section 1.13 – This definition basically includes all Protection Systems and Special Protection Systems operated at 300kV and above that if unavailable would have an Adverse Reliability Impact. Could not find a definition for “Adverse Reliability Impact”. We assume Adverse Reliability Impact to mean risk of instability, separation, or cascading failures per the High BES Impact definition. Per the NERC Glossary of Terms, Protection System is defined as “protective relays, associated communication systems, voltage and current sensing devices, station batteries, and DC control circuitry”. Recommend Protection System be removed from this definition; loss of a Protection System simply because it is above a specific voltage level does not cause BES instability, separation, or cascading failures. Recommend “Special Protection Systems” be changed to “non-redundant Special Protection Systems”. Also, suggest replacing “would have an Adverse Reliability Impact” with “would have an immediate adverse Reliability Impact such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures”. Attachment 1, section 2.2 - Recommend that this definition be removed entirely or moved to the Low Impact section; loss of individual Transmission Subsystems simply because it is above a specific voltage level does not affect the capability of the BES. Attachment 1, section 2.5 - This definition basically includes all Protection Systems and Special Protection Systems operated at less than 300kV that if unavailable would have an Adverse Reliability Impact. Could not find a definition for “Adverse Reliability Impact”. We assume Adverse Reliability Impact to mean risk of instability, separation, or cascading failures per the High BES Impact definition. Per the NERC Glossary of Terms, Protection System is defined as “protective relays, associated communication systems, voltage and current sensing devices, station batteries, and DC control circuitry”. Recommend Protection System be removed from this definition; the current wording would cause all protective relays operating at less than 300kV and above 100kV (per definition of Bulk Electric System) to be in scope without any regard to a real impact on the BES. Also, suggest replacing “would have an Adverse Reliability Impact” with “would have an immediate adverse Reliability Impact such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures”. The term “aggregate” is not defined in Attachment 1. For plants with multiple units this would imply that the combined output of all units should be considers as a single Generation Subsystem. There is no delineation for consideration of units, which are not interconnected by common cyber systems. This delineation should be included. Consideration should be provided to allow a Generation Subsystem to be classified as either a Medium BES Impact, Low BES Impact or a proposed No BES Impact system where supported by the identified evaluation or assessment method. Rational for the threshold values of 2,000 MVA and 1,000 MVA should be provided to assist in the analysis. Consideration should be provided to allow a Generation Subsystem to be classified as either a Medium BES Impact, Low BES Impact or a No BES Impact system where supported by an engineering study.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Blackstart units are required to start during periods without available offsite power, this would most likely preclude the use of cyber connectivity. The requirement that the connectivity not constrain operation is probably better covered under another reliability standards scope. Attachment 1 Criteria 1.8 states “including as notified by the Generation Owner.” Should this be “as notified by the Generation Owner.”?
AEP	The functional approach for determining impact categories would provide the opportunity to clearly define what is most important and what needs the greatest attention. It’s important to recognize that most any system is designed to continue to operate successfully, even under conditions where some parts are not optimally functioning. The factor of how long can you continue with without certain components helps to prioritize the protection necessary. Also, many systems contain algorithms to address fault conditions and back-up components for failed occurrences. These factors don’t seem to come into consideration under the current draft standard approach.
Edison Mission	Attachment # 1 has many issues, a number of which have been presented in the paragraphs below according to their numbered paragraphs: 1.1 The arbitrary 2,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why “name plate MVA” rating has been designated versus “net output” based parameters. 1.3 Reliability “must run” units are frequently old units to be retired but held in an operational mode for MW capacity or VAR capabilities. Some regions are disbanding these unit designations. Accordingly, we do not believe that all “must run” designated units should categorically be included as High impact. 2.1 The arbitrary 1,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why “name plate MVA” rating has been designated versus “net output” based parameters. Lastly, we are not of the opinion that an interruption of this arbitrary value of generation necessarily will “directly affect the electrical state …..of the BES.” For example, EROCT has a Contingency Reserve of 2,300 MW. The term “capability” of the BES is not an appropriate provision, e.g., the loss of even 10 MW will impact the total “Capability” of the regional system, but this is not the intent of the standard.
Calpine	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Black start plants required for grid restoration would be considered High impact.
NS&T	We believe criteria should be simplified in order to avoid having the process of identifying high, medium, and low impact BES assets consume excessive amounts of time and effort.
Flathead	Eliminate Low BES Impact assets as by definition they are not critical. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at small LSE/DPs that didn't identify critical assets. The low impact methodology has the potential to affect small entities more than the ones this re-write should properly target.
E ON	The drafting team should clarify item 1.5 of Attachment 1. Does the 3 line criteria only apply to 300kV and above or any voltage transmission line. For example, would a substation with 345kV looped in and out and one 138kV line exit qualify as a "High BES Impact" asset? Similar comment for item 2.2 under Medium BES Impact. Also, Using TLR as a criteria for classifying a Transmission Subsystem as High BES Impact seems overly restrictive. TLRs are called for a variety of reasons (planned outages, unforeseen loop flows, weather impacts, etc.) that do not seem to be a very good indication of the criticality of an asset. The criteria of IROL as stated is the only criteria needed in item 1.7.
Carthage	Make sure that the criteria are as specific as possible to eliminate confusion. No specific comments for High BES Impact. Section 2.5 under Medium BES Impact states that Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300kV in the Eastern and Western Interconnections, or less than 200kV in other interconnections that have an Adverse Reliability Impact. CWEP feels that simply stating each protection system, special protection system or remedial action scheme operated at less than 300kV is too broad a range. We feel that this could be interpreted to mean every piece of protective equipment operated at less than 300kV including protective relays and other equipment on our distribution system that have no material impact on the BES. CWEP offers the following revision to 2.5 for consideration. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated from 100kV to 299kV in the Eastern and Western Interconnections, or 100kV to 199kV in other interconnections that have an Adverse Reliability Impact. CWEP feels that there should be criteria established for Low BES Impact and a category of No BES Impact added. CWEP has facilities that it feels should be evaluated in the categorization process but would not fit under any of the criteria established for High or Medium Impacts. We further feel that simply placing them in the Low Impact category because they don't fit in the High or Medium categories wouldn't be correct because they don't have any material impact on the BES. CWEP feels that not having a No BES Impact category would create a situation where entities leave facilities out of their assessment so that they don't have to implement any controls on those facilities.
WECC	see previous comments about ambiguity and passive language.
Entergy	Apply them appropriately. Hierarchical categorization of loss impact of individual electric operating sites/assets may be useful in defining physical security standards. But electric grid asset rating/size categorization is not salient to definition of hierarchical security control and

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	countermeasure requirements for cyber assets. Hierarchical sets of requirements (controls and countermeasures) are needed for cyber assets themselves, based upon how much risk they themselves pose to reliable operation of the bulk electric system should they be lost or compromised.
CenterPoint	In Item 1.5, one sees the implementation problem introduced by the "BES subsystem" classification. Since the entire Eastern interconnection is interconnected, for example, all 345 kV facilities and higher could be considered a Transmission Subsystem under 1.5. If this subsystem were "destroyed, degraded, or otherwise rendered unavailable", the BES would most certainly be unstable. The net effect of such an interpretation, which fits the definition of transmission system and the verbiage in 1.5, would be that every transmission asset rated 300 kV or higher in the Eastern Interconnection would be considered a "Critical Asset" or "High BES Impact" subsystem because it is part of the High Impact subsystem. Although the Eastern Interconnect is used as an example, the same result would be true for WECC and ERCOT. One could certainly argue that the entire system is by definition not a "subsystem". The question then becomes how much of the system should be considered a "subsystem"? Would all of FP&L's 300 kV and above facilities be considered one "subsystem"? Or would all 300 kV and above facilities in the state of Florida be one "subsystem"? Or all 300 kV and above facilities in SERC be one "subsystem"? Or is it somewhere in-between these illustrative examples? The point of this discussion is that the verbiage indicating facilities above 300 kV or 200 kV would not be considered "high impact" if an engineering evaluation indicated loss of the subsystem would not cause instability or voltage collapse appears to either be a red herring (because all such facilities could be part of a large enough "subsystem") or lead to differing opinions as to when a subsystem is too big to be considered one single subsystem. For this reason, CenterPoint Energy re-urges classification by asset, not by the proposed "subsystem" classification that is open to varying interpretations. Besides the rather large flaw discussed above in 1.5, which could be remedied by changing "subsystem" to "asset", item 1.5 also appears to have an arbitrary and inexplicably discriminatory distinction of 300 kV versus 200 kV facilities for the Eastern and Western interconnection versus other interconnections. CenterPoint Energy operates in the region that is the apparent target of the discrimination, ERCOT. Ironically, the distinction between 200 kV and 300 kV facilities within ERCOT does not matter because no transmission facilities operate in that range in the ERCOT region. Nevertheless, CenterPoint Energy encourages a non-discriminatory requirement, either at 200 kV or 300 kV. Items 1.4 and 1.6 are either overly broad or unreasonable. As the discussion of item 1.5 illustrates, the interconnected nature of the BES allows everything in it to arguably be construed as a "subsystem" and any subsystem at some point will be large enough to cause the failure of the entire system. In such a paradigm, creating "impact" based distinctions becomes meaningless and open to differing interpretations. The present standard requires consideration of black start units and assets within cranking paths. If a region has significant diversity of black start resources and diverse cranking path options for each resource, it is possible that any single, independent (no common element or cyber system with another black start resource) black start resource would not be "critical" or "high impact". Even if all black start resources are considered critical, a valid risk-based assessment would consider the diversity of cranking paths to ascertain whether assets in any given path would be "critical" or "high impact". The wording in 1.6 indicates all possible cranking paths would be high impact, which conceivably could be all or most of the network, yielding an illogical outcome. For example, a black start unit with three different cranking path options has many more options and is therefore more secure than a unit with only one cranking path. The facilities associated with three different cranking paths are much less critical and have much lower impact if damaged

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	than the facilities associated with one single cranking path. However, ironically, many more assets would be classified as “high impact” or “critical” under the scenario where there are three available paths than the scenario with only one path, a completely illogical result. At a minimum, CenterPoint Energy recommends revising 1.6 to criteria based upon diversity of cranking paths, such as designating as cranking path assets as critical until a threshold number of different paths are available, such as two or three. CenterPoint Energy recommends deletion of 1.7. This criterion diverges from the alleged definition of high impact facilities. Violating an IROL is a different standard from the criteria of instability, cascading outages or voltage collapse. Applying 1.7 would cause all or virtually all facilities to be considered high impact, negating the exercise of attempting to distinguish high impact or critical facilities from other lower impact, less critical facilities. CenterPoint Energy also recommends deletion of 1.9. Certain facilities may be pertinent from the standpoint of providing, say, off-site power to a nuclear power plant, but such facilities may not have a significant BES reliability impact. Moreover, NUC-001 requirements relating to concepts such as maintaining steady state switchyard voltage in a certain range would be open-ended if put into the context of proposed item 1.9 because voltage at a nuclear plant interconnection switchyard depends upon the cumulative effect of the entire transmission network and the generators connected to it. NUC-001 is specifically designed as the appropriate standard to address such issues, not CIP-002. Indeed, to the extent that certain aspects of CIP-002 might be relevant to certain aspects of nuclear plant operations, the nuclear plant operator can address the issue by providing the applicable reference to CIP-002 through a Nuclear Plant Interface Requirement as outlined in Requirement R1 of the NUC-001-2 standard.
LCRA	1. Attachment 1, 1.4 – This is not clear. Does this only include the primary blackstart units or does it extend to any unit mentioned in the plan for any reason? 2. Attachment 1, 1.5 – This needs to be more clearly defined. The three or more transmission lines leaving the station need to be defined as also being operated at or above the 200 or 300 kV voltage levels. 3. Attachment 1, 1.6 – The current definition of cranking path in the Glossary is too general to be used in this statement. The sentence would better define the path as follows: “Each Transmission Subsystem comprising the primary Cranking Paths between the primary blackstart units and the next start units.” 4. Attachment 1, 1.16 – What is the definition of “transmission assets of 2,000 MW or more”? Does this mean transmission serving 2,000 MW of load or transmission lines capable of carrying 2,000 MW of power? 5. Attachment 1, 2.2 – This needs to be more clearly defined. The three or more transmission lines leaving the station need to be defined as also being operated at or above the 100 or 200 kV voltage levels.
FRCC	The use of the term "degraded" is used in many of the identified assets (1.7,1.10,1.11, 1.12 and more). As previously mentioned, this term can mean many different things and it will likely result in interpretation requests. The drafting team should try to be clear what impact they really want to be considered and be specific in the language.
NIPSCO	Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities’ obligation. Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	aggregate load shedding capability or to the single step load shedding increment. There seems to be inconsistency in the use of MW vs. MVA We believe that the standard shouldn't use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement similar to MOD-024-1
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A-10 Criteria. Also it is recommended the standard raise the requirement of the 300 MW of automatic load shedding. This value should be 500 MW.
EEI	Proposed amendments to Attachment 1 were provided earlier.
O&R	NERC should consider that certain entities may have facilities that fall under the BES definition for a given region, but because of their own system's characteristics, do not have an impact on the Interconnected BES. There should be an additional category of NA, as with other NERC Reliability Standards. Since the NERC standards apply as per the entity's registration, the entity would then need to provide evidence as to how they categorized the BES subsystems. If all/any BES subsystem elements that are not High or Medium are simply categorized as low, depending on what requirements CIP-003 - 009 bring forward, there could be undue and unjustified entity/consumer costs associated with implementation on BES elements that really do not require such. The Drafting Team should consider use of an impact-based methodology such as the NPCC A-10 Criteria. Also it is recommended the standard raise the requirement of the 300 MW of automatic load shedding. This value should be 500 MW.
Alliant	We believe Item 1.2 should include "for the Contingency Reserve Sharing Group" at the end of the statement to make the intent clearer. In Item 1.2, the term "Reserve Sharing Obligations" should be defined in the NERC Glossary of Terms. In Item 1.3, the term "Reliability must run units" should be defined in the NERC Glossary of Terms. Under Item 1.4, we believe this represents the same "one size fits all" approach that the Guidance for the Electric Sector: Categorizing Cyber Systems document claims to be trying to eliminate. In reality, not all blackstart Generation Subsystems listed in the Regional Restoration Plan carry the same weight, or have the same impact on the region, so it seems like a hierarchy should be developed within the standard for categorizing these units as either High, Medium, or Low Impact. We feel this hierarchy should be based on the size of the Generation Subsystem (similar to the delineation defined by CIP-002-4 Attachment 1, Sections 1.1 and 2.1, but not at the same MVA level), as well as the Generation Subsystem's impact on the Regional Restoration Plan, such as if it has a role in cranking support for a nuclear plant. Item 1.4 does not differentiate between a utility having numerous blackstart capable Generation Subsystems, where failure of multiple blackstart Generation Subsystems would not compromise their entire blackstart plan, or a utility with a single blackstart Generation Subsystem that is then essential to the success of their blackstat procedure. A utility should be given consideration for having multiple blackstart Generation Subsystems, which makes their blackstart plan inherently more reliable, not penalized for it. In Item 1.10 we propose to replace "in voltage collapse" with "in voltage collapse that would pose and unacceptable risk to the Adequate level of Reliability to the BES.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	In Items 1.16 and 2.6 we do not believe transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
Ameren	1.1 Deliverable MW should be used rather than the nameplate MVA for the generation subsystem. 2000 MW is an appropriate threshold for the high BES impact. 1.3 Generators designated as RMR to prevent IROL or are needed to prevent the loss of over 300 MW of load should be included as "high". RMR generators that are needed to prevent loss of load of less than 100 MW should be considered as low BES impact, and for loss of load of 100 to 300 MW should be classified as medium BES impact. 1.4 Only the black-start generators that are in the Regional Restoration Plan and are integral to system restoration should be candidates for high impact. Other black-start units should be considered as medium impact. Use EOP standard for criteria for system restoration. 1.5 Use criteria from EOP for system restoration so that all black-start units and all cranking paths are not considered high impact. 1.6 All transmission substations in all Cranking Paths do not qualify for high impact. Only those substations in Cranking Paths that are integral to System restoration should be included as high. The substations in other Cranking Paths should be considered as medium or low. Use EOP standard for criteria for system restoration 1.7 Remove “or exceeding limits requiring transmission loading relief (TLR)” 1.8 Remove “including as notified by the Generator Owner” Remove 1.10, 1.11, and 1.12 1.13 Added language “associated with” after “each protection system” 2.1 Similar to 1.1 above, deliverable MW should be used rather than the nameplate MVA for the generation subsystem. 1000 MW is an appropriate threshold for the medium BES impact. 2.3 This statement should be modified to replace section 2 with section 2.1. 2.5 Our view of this language makes all Protection Systems of less than 300 kV as medium impact. SPS that pass TPL-003 and TPL-004 requirements should not be included.
Black Hills	In Attachment 1, Section 1.2 on RSG obligations - need clarification of whether 'obligation exceeded' refers to that required by a single entity, or the total of all entities in the RSG. For consistency, the impact evaluation of a BES Subsystem be done by an RC.
TNMP	The criteria needs to have a means of addressing jointly-owned BES Subsystems, as mentioned in the comments for number four regarding requirement R1. Another significant concern is the requirement for engineering studies called for in the High Impact. To successfully pass an audit, a Responsible Entity would need to perform engineering studies on all Transmission Subsystems. TNMP sees this approach as casting too wide a net with little incremental return. TNMP believes the engineering studies in 1.10 through 1.12 should have the following constraints: -A Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections with 3 or more transmission lines leaving the station.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	-Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. -Excluding any Transmission Subsystem that has already been identified as High Impact based upon other matching criteria. These constraints would limit the scope of studies to determining if a Medium BES Impact station should actually be a High Impact. It also eliminates the need for engineering evaluations being performed for compliance purposes on stations that are already defined as having a High Impact.
NVEnergy	Suggestions for improving proposed criteria: Comments on specific sub-items as indicated below: 1.1 The 2000MVA threshold appears on the surface to be a reasonable breakpoint for designation as High Impact; however, the use of a fixed value may not adequately account for the relative sizes of various Balancing Areas and Interconnections. 1.2 This item could use some additional clarity. What does it mean to have output that exceeds the Contingency Reserve or total Reserve Sharing Obligations? Obligations of whom? As an example, if a BA has an obligation share to its reserve sharing group of 75MW in a particular hour, does that imply that any generating unit larger than 75MW is High Impact? This is out of line when compared with the 2,000MVA level indicated in 1.1. 1.3 For Reliability Must-Run unit designation, the standard must clarify that the reliability scope is of the BES, not the local distribution, for instance. Also, it is unclear who would make such designation. 1.4 As noted in response to #2 above, the importance and criticality of Black Start facilities are being over-stated by placing them in this category. 1.5 Clarity is needed in the definition of transmission lines. Does this term include only the elements that function as transmission lines, or does it also include radial feeds, station positions that interconnect generator step-up transformers, or other transformer connections? What is driving the threshold of 3? 1.6 As with blackstart generators, the inclusion of the Cranking Path facilities in this category is inappropriate. 1.13 More precision is needed in this language, which currently categorizes Protection Systems, SPS or RAS “operated at 300kV and above” as High Impact. None of these systems operate at high voltage; what was intended was to refer to the BES systems that they protect operate at 300kV and above. As well, how does an entity determine if the destruction of such SPS would have “Adverse Reliability Impact”? What degree of impact is allowable? 1.14 A departure from the CIP-002-1,2,3 Standards in this version 4 removes the qualifier that the 300MW load shedding system is under a common control. Is this language intended to capture discrete underfrequency load shedding relays that are sprinkled throughout an entity’s distribution system? If so, this reaches too far. 1.16 The size threshold of system controlled by a BA/TOP control center is proposed at 2,000MW. Is this value a transmission capacity number, generation capacity number, or total system/area load value? If load, is it the historical peak, forecast peak, average over the peak season, other?
MWDSC	If an engineering evaluation demonstrates no Adverse Reliability Impact of any interconnected BES, add another category such as "No BES Impact" or a subcategory of Low BES Impact with limited application of unknown security requirements in CIP-003 through CIP-009.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Add a guideline at the same time as standard is completed such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Need to show Bright lines. Black start units are defined differently in different regions. The RC should determine who's BS unit has a high impact on the BES based on RC study. Merely listing a unit as a BS unit does not necessitate it as a high impact to the BES. For example some BS units can be a 5kw gas engine in a metal shed and another's may be a 20MW CTG or a hydro unit in a dam, yet all would, according to the proposed standard have the same High impact to the BES and this seems wrong in nature. It would be best for the RC to determine these High impact BS units based on regional studies to what is important for the region. People with multiple blackstart units are tempted to remove those from the current regions plan in order to be compliant with the proposed standard, hence undoing reliability of the BES in order to show compliance with the standard. A different approach is needed.
NCEMCS	As stated many times "Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009, or a category for minimal-risk or no-risk subsystems must be created!"
SWTC	There is not much in the proposed standard that provides sufficient guidance on how to designate a transmission or generation subsystem. The emphasis appears to be mostly on determining whether the transmission and generation subsystems - to the Bulk Electric System (BES) - have a high, medium, or low impact. Attachment 1 to the proposed CIP standard tries to set some guidelines for transmission and generation for high and medium BES impact, but then lump the rest into the low BES impact.
SCEG	Beneath the Impact level categorization items should be more clearly grouped based on subsystem type. The SDT should also define Protection Subsystems.
Exelon	As stated previously Exelon supports the use of Attachment 1 as the primary tool for the categorization of system/subsystem elements. We ask that the criteria listed in attachment 1 be evaluated and revised to remove any ambiguity and technical justification be considered as a primary factor for setting the criteria.
BPA Trans	Suggestions for improving proposed criteria: This needs to be simplified. All of the criteria (1.7, 1.8, 1.10, 1.11, 1.12, 1.13, and 2.3) that includes the statement "if destroyed, degraded, or otherwise rendered unavailable, would" should be removed. There are enough criteria identified for High, Medium and Low BES impact without adding those elements that requires additional work not done today to answer. We are trying to increase reliability by having multiple cranking paths. But in doing so, it appears we are being penalized for identifying more cranking paths via these criteria. It seems sensible that robustness and redundancy should weigh into the criticality of an asset and this should be included this in this criterion.
HQT	Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. • The detailed Attachment 1 definition does give clarification. In any system where the Contingency Reserve is less than 2000 MW, clause 1.2 dominates clause 1.1 so engineering evaluation cannot be used to reclassify a Generation Subsystem into having a

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Medium BES Impact. Just because a Generation Subsystem is classified as Reliability "must run" doesn't mean the system can't survive if it fails (has a forced outage). Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. Request clarification on the wording "leaving" in 1.5. Also, 1.5 should be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station… Request clarification where 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include distribution necessary to complete the cranking path? Why are blackstart related systems "High BES Impact"? The electric system has already failed when the "blackstart related systems" are needed. 1.10, 1.11 and 1.12 should be removed and language added to 1.7 as follows: Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs)or SOLs for those areas that do not identify IROLs, or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method. Request clarification on 1.13, which SPS 300 kV threshold (550 kV for the Quebec Interconnection), sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. Also, 1.13 should be made to read: Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact. Request clarification on "automatic load shedding" in 1.14. If this refers to under-frequency load shedding then Distribution Provider must be added to the Applicability Section. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center" Request clarification on wording "leaving" in 2.2. Also, 2.2 should be made to read: Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, 300 kV or higher for Quebec Interconnection or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station… Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add ", including as notified by the Generation Owner" Consistent with 1.9, recommend changing 2.4 from "NUC-001-1" to "NUC-001" Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. Also, 2.5 should read: Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, less than 550 kV for the Quebec Interconnection or less than 200 kV in other Interconnections that have an Adverse

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Reliability Impact. Consistent with the comment on 1.15 and 1.16, recommend changing from “Control Center and backup Control Centers” to “Primary Control Center and any backup Control Centers” in 2.6. Attachment 1 does not belong in a CIP document. Once implemented these definitions are likely to receive broad application.
Allegheny Energy	- Resolve the confusion of terms used in the proposed glossary additions. - Item 1.1 - What is the rational for 2,000 MVA value? (Why not 2,500 for example.) What would an example of an approved engineering evaluation be? - Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities’ obligation. - Item 1.13 - “Adverse Reliability Impact” and other locations should be changed to “Adverse BES Reliability Impact.” - There seems to be inconsistency in the use of MW vs. MVA
KCPL	The criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to “plug into” this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
Connectiv Energy	High, Medium and Low categories are adding a potentially unnecessary level of complexity. Transmissions Operators (TOPs) such as PJM which are concerned with and track such things as “contingency reserve”, “reliability must run” status, “Nuclear”, “voltage support” requirements, resulting “interconnect reliability operating limits” upon loss of a unit, and “black start” designations for the units in its system. As these are important to PJM for the operation of its grid, we as Generator Owners (GOs) and Generator Operators (GOPs) have used these as guides in determining which of our units are critical and would prefer not to have the FERC directly impose different requirements, but to work with the TOPs to reasonably influence criteria to be used in determining critical status.
MidAmerican	Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, MidAmerican recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) in question 13, but moving the categorization aspects of CIP-002-4 into the development work with security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. To demonstrate, see the following

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	examples. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might be on the list as one, but not the only, acceptable method to achieve the objective of low electronic authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161 kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. If the security controls developed support the need for categorizations based on concepts in Attachment 1, the attachment should strive to eliminate the need for creating new definitions and concepts for these subsystems. Attachment 1 is hindered by the issues identified with the confusing definitions for Generation Subsystem and Transmission subsystem. Where meaningful categorizations are identified, their criteria should be bright line. MidAmerican recommends bright lines that do not necessitate engineering analyses or third party review. Bright line examples for substations would be substations with highest voltage connected at: 100-199kV are categorized as low, 200-299kV are medium and at or above 300kV are high. Substations connected at with highest voltage under 100kV are only in scope if they are part of the primary black start path. Bright line examples for generating units are units: rated at 100-299MW are categorized as low, 300-499MW are medium and at or above 500MW are high, as long as the unit is connected to the system at 100kV or above. Generating units under 100MW and/or connected to the system at under 100kV are only in CIP scope if the unit is a primary black start unit. Wind farm generating units are not in scope where the reliability of the BES is not designed to be dependent on the wind blowing.
CPG	For Item 1.2, what does the term "aggregate output" mean? Is that forcing GO/GOPs to evaluate their plants on an aggregate basis, even though they are separate Subsystems? For clarification, the wording should state "the MW or MVA output of the Generation Subsystem" so not to confuse the aggregate output of a plant with the aggregate output of the Generation Subsystem. For Item 1.5, who is the Reliability Assurer? For Item 1.5, it is common for a GO/GOP to communicate the impact levels of their assets to their interconnected

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	TO/TOP, and vice versa. This is an excellent means to ensure the reliable operation of the Bulk Electric System.
Santee Cooper	Suggestions for improving proposed criteria: Simplifying the list. It seems to inter-mingled with Attachment 2. SC believes in the approach of determining which assets are critical to the reliable operation of the BES first, then assigning impact levels. For example, Blackstart units may not end up on the high impact list because of multiple cranking paths.
OGE	• 1.1 – if the Subsystem is "not essential to the reliability of the BES", why do these systems retain the overhead associated with the Medium BES Impact? This is essentially saying "all Gen Subsystems with aggregate name-plate generation >= 2,000 MVA will be "High BES impact", unless you prove they are not essential… then you can drop them down to "Medium BES Impact". • In 1.1, "aggregate rated name-plate" is used and in 1.2 "aggregate output" is used. For consistency, should both state "aggregate rated name-plate". If not, 1.2 should state net output if that is the intent. • 1.4 – Needs to more specifically indicate "designated Blackstart Resource" per the regional blackstart capability plan. It should be noted that non-designated units may be referenced in the plan which could be construed as "included in the plan" {Reference EOP-005-2 R1.4} • 1.5 – Is it a subsystem that "contains" switching stations or are the switching stations themselves a Transmission Subsystem? • 1.5 - Lines "leaving the station" gets into direction of power flow. It appears the intent is lines "terminate (or intersect) at the station". • 1.5 – No indication that "…in which case…" these can be dropped to "Medium BES Impact" like 1.1, yet in 2.2, it indicates "not already included in section 1 above…" • 1.6 – Not clear what is intended by "Cranking Path". Should this be "Blackstart Cranking Path as designated in the regional blackstart capability plan or regional blackstart restoration plan? • 1.6 – Need to designate additional criteria, such as a threshold or the "primary" or "initial" cranking path, to include Transmission Subsystems in the "cranking path". In some cases several alternate cranking paths may be provided and it is counterproductive to include all alternate paths. • 1.10, 1.11 - Reference other standards that define the criteria / voltage collapse (TPL standards). • 1.12 - Use "BES" in place of "transmission system"? Wording makes criteria difficult to follow. Should "Adverse Reliability Impact" be used in place of "… or separation of Cascading outages."? • 1.12 - Is the intent for this to be "as determined through an engineering evaluation or other assessment method"? Should indicate an "approved" method for consistency? • 1.16 – Is the intent of the statement "… functions for transmission assets or generation assets of 2,000 MW or more." It is not clear in terms of transmission assets. First, this seems to deviate from the "MVA" ratings used earlier. Second, the phrasing no longer uses terms used earlier in the document such as "Transmission Subsystem" or "Elements". If the statement is specifying any transmission asset, it should state that (e.g. "… functions for any transmission assets…". If it is specifying transmission

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	assets of 2,000 MW or more, it is not a clear method to describe transmission assets. • 2.5 – This category appears to be incomplete. Should this include the same statement as 1.13; "…that, if destroyed, degraded or otherwise rendered unavailable, …" ?
Oncor	Item 1.9, we propose to change "essential" to "required". Item 1.10, we propose to replace "in voltage collapse" with "in voltage collapse that would pose an unacceptable risk to the Adequate Level of Reliability of the BES". Item 1.12, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 1.13, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 1.16, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided. Item 2.4, we propose to change "essential" to "required". Item 2.5, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 2.6, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
PPL Supply	See response to #4 above.
St. George	As a small municipality, we applaud the draft team for dealing with the over-simplistic classification of an asset as Critical or Non-Critical. The proposed standard takes two classifications (Critical and Non-Critical) and makes three (High, Medium, and Low). We are deeply concerned that three classifications are not sufficient to represent the true nature of the BES. At minimum another classification should be added: Minimal. This would be for Generation Subsystems below 200 MVA and transmission below 150 kV in the Eastern and Western Interconnections. Low would then be for Generation Subsystems of 200 – 1,000 MVA and transmission of 150 – 200 kV in the Eastern and Western Interconnections. The Minimal classification assets would then be exempt from CIP-003 through CIP-009 in the same way Non-Critical assets are currently.
NGRID	• Suggestions for improving proposed criteria: • Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. • To distinguish between "must run" and "Reliability must run", recommend that 1.3 change from "must run" to "Reliability must run" • Request clarification on "leaving" in 1.5 • Request clarification are 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include distribution

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	necessary to complete the cranking path? • Recommend removing 1.10, 1.11 and 1.12 since none have an explicit threshold and is redundant with 1.7 plus does not provide enough details on who does these engineering studies or how they conduct such studies As per the discussion, it was noted that the redundancy of 1.10, 1.11, and 1.12 is because some areas do not have IROLs. In such a scenario, following is recommended If 1.10, 1.11 and 1.12 exist to plug gaps in IROLs, then they should be sub bullets of 1.7 and start with something like "For those areas that do not use IROLs …" If 1.10, 1.11 and 1.12 remain; they need to address our concerns about "explicit threshold" and "who/how on the engineering studies" - Alternatively, number 1.13 (Protection System, SPS and RAS) needs to be deleted because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) • Request clarification on "automatic load shedding" in 1.14? If this refers to under-frequency load shedding then it may include distribution. • Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center" • Request clarification on "leaving" in 2.2 • Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add ", including as notified by the Generation Owner" • Consistent with 1.9, recommend changing 2.4 from "NUC-001-1" to "NUC-001" • Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. • Consistent with the comment on 1.15 and 1.16, recommend changing from "Control Center and backup Control Centers" to "Primary Control Center and any backup Control Centers"
MGE	MGE does not support the three level approach. MGE would support a four level approach that has the addition of a "No BES Impact" category. This category would contain such cyber assets as contained in a Registered Entity's UFLS program or assets that don't currently impact the BES. The purpose of the UFLS program is to provide a last resort for system preservation. It is not defined in the UFLS Standards that the UFLS program is to maintain BES stability, but that is why there is a UFLS program. By not having a No BES Impact category, the SDT is not giving a bright-line solution for those entities who are only DP's with UFLS programs, etc.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
FE	In general we disagree with the H/M/L classification driven by Attachment 1, and in particular some of the classifications between H/M seem arbitrary, especially the size of generation subsystems. We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. As presented, we believe Attachment 1 could be improved by eliminating 1.10, 1.11 and 1.12 which are redundant with 1.7.
TECO	We support EEI's comments regarding attachment 1.
Snohomish	We have a concern with the MW thresholds that are used and that they do not actually identify impact risk. We prefer a more performance-based approach for both loss of load and generation, such as a utility or region cannot adversely impact neighboring systems.
CECD	2000/1000 MW or greater. - Nameplate rating should not be used to determine impact categorization, but rather actual tested capacity should be applied so that the real risk to the interconnection is examined. Furthermore, guidance indicates that a Generation Substation can be divided up into its components so it is not clear whether this will be interpreted the same way. Specifically, the guidance document states "The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. For example a multiple unit generation facility can be defined as one or more Generation Subsystems depending on the functions being performed and the operational and technical characteristics of the generating unit." It is not proper to include frequency support as a factor for consideration in determining whether a unit is essential to the reliability of the BES. It is not clear how frequency support would be determined? For example, the loss of a 500 MW in the WECC footprint will have a much greater impact to frequency than the loss of the same unit in the Eastern Interconnection. In the Units larger than the Reserve Obligation criteria, is aggregate output referring to actual tested capacity? It is not appropriate to include a control center in the BES Subsystem category. A control center is more appropriately considered a Cyber System to be evaluated in relation to a BES Generation or Transmission Subsystem. Furthermore, language relating to control centers in Attachment 1 should use the term BES Transmission Subsystem and BES Generation Subsystem. It should also be clear whether the ratings apply to individual subsystems or all BAA subsystems in aggregate. There is a delicate balance between regulation supporting reliability measure and creating disincentives that may, in practice, reduce reliability. These standards must thoroughly consider the implications of imposing requirements to achieve reliability improvements not to hinder current reliability practices
MRO	We feel Attachment item 1.2 should include "for the Contingency Reserve Sharing Group" at the end of the statement to make the intent less ambiguous. Under Attachment item 1.2, we also feel the term "Reserve Sharing Obligations" should be defined in the NERC Glossary of Terms. Under Attachment item 1.3, we feel the term "Reliability must run units" should be defined in the NERC Glossary of Terms. Under item Attachment 1.4, we feel this represents the same "one size fits all" approach that the Guidance for the Electric Sector: Categorizing Cyber Systems document claims to be trying to eliminate. In reality, not all blackstart Generation Subsystems listed in the Regional Restoration Plan carry the same weight, or have the same impact on the region, so it seems like a hierarchy should be

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	developed within the standard for categorizing these units as either High BES Impact, Medium BES Impact, or Low BES Impact. We feel this hierarchy should be based on the size of the Generation Subsystem (similar to the delineation defined by CIP-002-4 Attachment 1, sections 1.1 and 2.1, but not at the same MVA levels), as well as the Generation Subsystem's impact on the Regional Restoration Plan, such as if it has a role in cranking support for a nuclear plant. Attachment Item 1.4 currently does not differentiate between a utility having numerous blackstart capable Generation Subsystems, where failure of multiple blackstart Generation Subsystems would not compromise their entire blackstart plan, or a utility with a single blackstart Generation Subsystem that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple blackstart Generation Subsystems, which makes their blackstart plan inherently more reliable. Under Attachment item 1.5, to remove ambiguity we feel we should replace "switching stations" with "switching stations or substations". Attachment Item 1.6 currently does not differentiate between a utility having numerous Cranking Path options, or a utility with a single Cranking Path that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple Cranking Path options, which makes their blackstart plan inherently more reliable. Under Attachment item 1.9, the lack of a definition for "essential" makes this statement ambiguous. Under Attachment item 1.10, we propose to replace "in voltage collapse" with "in voltage collapse that would pose an unacceptable risk to the Adequate Level of Reliability of the BES". Under Attachment item 1.12, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Under Attachment item 1.13, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Under Attachment item 1.16, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided. Under Attachment item 2.2, to remove ambiguity we feel we should replace "switching stations" with "switching stations or substations". Under Attachment item 2.4, the lack of a definition for "essential" makes this statement ambiguous. Under Attachment item 2.5, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Under Attachment item 2.6, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
GTC	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
Xcel	We would like to see a category of 'no impact' for systems with no outside connectivity.
BGE	Consider the establishment of a reliability-based "Bright-line" methodology to remove ambiguity and assure the standard is applied

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	consistently throughout the industry. Also, an alternative proposal to Attachment 1 is given in our response to Item #3.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Suggestions for improving proposed criteria: Regarding High BES Impact 1.1, we believe approving assessment methods should be the function of the Regional Entity and/or NERC and the roles of the RC will need to be explicitly defined. In cases where the RC function has been delegated to a utility agent, we feel controls should be in place to avoid conflict of interest and/or shield the agent from liability. Regarding High BES Impact 1.2, we suggest striking this criterion. Independent Generators do not have access to the information described in 1.2 and therefore cannot assess their Generator Subsystems appropriately. We also suggest striking the term “Adverse Reliability Impact” as it is not defined in the Glossary of Terms. We also suggest amending the standard to filter only for those Generators that are “primary blackstart.” Many generators may be included in a restoration plan, but are of secondary or tertiary value and not all blackstart units are equal.
TAPS	See TAPS response to Question 1.i.
Allegheny power	AP is in agreement with EEI’s amended Attachment 1.
FMPA	High BES Impact (H): FMPA recommends that criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region). The EPAct, FPA Section 215(a)(4) defines “reliable operations” as: “operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements," so, to boil it down, the EPAct passed into law mandatory standards to regulate the industry in its efforts to avoid "instability, uncontrolled separation, or cascading failures" This definition of "reliable operation" is nearly synonymous with the NERC Glossary term for "Adverse Reliability Impact": "(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." "Cascading" is further defined by the NERC Glossary as: "The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies." The focus of the standard ought to use this concept of Adverse Reliability Impact to define what is High risk, Medium risk and Low risk. Supply/Demand Mismatch and IROL: Starting from this theoretical basis, what kinds of conditions can cause an Adverse Reliability Impact, such as widespread frequency related instability? The answer really is a large mismatch of supply and demand (even faults can cause instability by "shorting out" the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	load, causing a large mismatch of supply and demand) or operating conditions, regardless of cause, that lead to violation of an Interconnection Reliability Operating Limit (IROL). Therefore, the entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs. The rest of Attachment 1 is simply a restatement of conditions that can cause these metrics to be exceeded. IROL is defined in the NERC glossary as: "(a) System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." IROLs are determined by study by the PAs and TOPs and these metrics are readily available in accordance with FAC-014. Hence, the only metric that remains to be established is the supply/demand mismatch. This mismatch can be caused in a few ways: 1. Tripping a large amount of generation through malicious use of cyber systems 2. Tripping a large amount of load due to malicious use of cyber systems to directly trip the load (e.g., use of a large SCADA system to activate a centralized UFLS system). 3. Tripping key transmission Facilities by malicious use of cyber systems that could cause voltage instability, thermal cascading, etc., that could in turn result in a large mismatch of supply and demand, the large mismatch of supply and demand being the key. (For example, the Northeast Blackout of 1965 was caused by loss of tie lines importing power from Canada causing a large supply/demand mismatch, and the Blackout of 2003 was caused first by thermal cascading, which in turn caused a voltage collapse of Cleveland and Detroit, which then resulted in a huge supply /demand imbalance through the loss of two major urban centers) FMPA recommends that the SDT develop a metric for supply/demand mismatch (e.g., the Contingency Reserves of the region, or another metric determined by study) that correlate with High and Medium Impact. High Impact should include those events that have a relatively high chance of causing an Adverse Reliability Impact, e.g., cause an IROL to be exceeded or a supply / demand mismatch greater than a certain metric. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 2000 MVA may be an acceptable default value for High Impact in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for the region. 1000 MVA may be an acceptable default value for Medium Impact in the absence of a specific regional threshold based on the largest single contingency for a PC or RC. Blackstart and Cranking Paths: If a wide-spread outage were to occur, utilities need to be assured that their blackstart units and cranking paths to other generators that are identified in the regional restoration plan will be available, and that the control systems for these devices have not been compromised. FMPA understands the need for protection of the “critical units” and “critical paths,” but the identification of all blackstart units as High Impact is not reasonable or necessary to ensure BES restoration. FMPA recommends that the categorization of blackstart units and transmission cranking paths between the blackstart units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, “High Impact” from a restoration perspective should focus on preventing restoration efforts and “Medium Impact” should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent blackstart efforts from multiple blackstart units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder blackstart efforts from a single blackstart unit or cranking path in

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	the regional plan. Blackstart capable units that are not in the regional plan should be Low Impact. Recommendation of Edited Language to High BES Impact: 1. High BES Impact (H) 1.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the Contingency Reserve or total Reserve Sharing Obligations of a Reserve Sharing Group or, if no Contingency Reserve or total Reserve Sharing Obligation has been established, a supply loss of 2000 MVA or a load loss of 2000 MW. 1.2. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.3. A BES Cyber System, that if maliciously used, can result in exceeding one or more Interconnection Reliability Operating Limits (IROL's). 1.4. A BES Cyber System, that if maliciously used, can prevent blackstart restoration efforts from multiple black start units and cranking paths identified in the regional restoration plan. FMPA believes using the above criteria would make Attachment 1 very simple, resulting in only four criteria instead of the 16 in the "High Impact" list proposed by the SDT. Most of the 16 items in the "High Impact" list are simply phenomena that can cause supply/demand mismatch greater than the established metric, or an IROL to be exceeded (e.g., voltage collapse, thermal cascading, loss of situational awareness, etc.) We recommend including these phenomena as subsections of the four criteria spelled out above. We believe such a method is much simpler to understand and enforce, and is more in line with what ought to be regulated - phenomena that can cause an Adverse Reliability Impact. If the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC. Recommendation of Edited Language to Medium BES Impact: Medium Risk should be those events that would put the system dangerously close to an additional contingency causing an Adverse Reliability Impact, e.g., an event that could cause a supply / demand mismatch greater than the largest loss of source that would put the system in a status whereby a single contingency could cause a supply / demand mismatch greater than the Contingency Reserves of a reserve sharing group, or an IROL to be exceeded, (at a point only a single contingency away). Also, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 1000 MVA/1000 MW for the Medium BES Impact threshold. 1000 MVA may be an acceptable default value for the Medium BES Impact threshold in the absence of a specific regional threshold based on the largest single source contingency. 2. Medium BES Impact (M) 2.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the single largest loss of source contingency of the region, or, if no single largest loss of source value has been established, a supply loss of 1000 MVA or a load loss of 1000 MW. 2.2. A BES Cyber System, that if maliciously used, can result in a system state whereby the next single contingency would cause the BES to exceed an IROL.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	2.3. A BES Cyber System, that if maliciously used, can hinder regional blackstart restoration efforts by preventing blackstart from a single black start unit and cranking path identified in the regional restoration plan. Low BES Impact (L): Low Impact should include all other BES systems that have a low risk of contributing to an Adverse Reliability Impact. FMPA cautions the SDT that even though the Low BES Impact category will have the least impact to reliability, it will have the most burdensome and widespread impact on registered entities for compliance purposes. We cannot stress this point enough; the industry needs assurance that the Low BES Impact requirements will be reasonable, and preferably, no requirements since it would seem beyond the scope of the FPA. If there are any requirements in CIP-003 and higher for Low Impact cyber systems, those requirements must be aligned with the cyber system protections that are programmatic in nature and are not cyber system specific. These requirements should be similar to the current CIP-002, which require a risk based assessment methodology where entities can manage compliance through employee training on the security of cyber assets, etc. Making the compliance requirements exceedingly strict will take valuable resources away from the protection of the high and medium impact assets. The industry's first priority should be to protect and secure the high and medium impact facilities.
Duke	Attachment 1 is not needed for the "Cyber First" approach. Any Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact, and protected accordingly.
NBSO	Considerations for improving proposed criteria: 1.1: Simply use a threshold number of 2000 MVA. Do not have the RC/RA held responsible to omit a generator. Alternatively I would see that the RC may overrule and provide a lower value threshold if necessary. 1.2: The "largest value of Contingency reserve" is not clear. Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. Suggest using a percentage of largest contingency to protect against those times were the typical largest contingency is reduced. 1.3: Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. A system must be planned and operated considering the loss of the must run unit regardless if a cyber incident or equipment malfunction. There appears to be overlap in 1.5, 1.8, 1.10, 1.11, 1.12 There should be some attempt to be more crisp, focusing on eliminating those situations where there is a increased risk to the bulk system due to the risk of exceeding credible contingency assumptions. Some of these are part of these items are in the SOL definition, so why not use SOL? 1.13: Needs clarity. Should consider all SPS's that would impact the BES. These could operate at a lower voltage then those listed. 1.14: For smaller areas the 300 MW threshold may be too large. Consider allowing RC input to lower this value. 1.16: "Transmission assets of 2000 MW or more" should be better defined. "Generation assets of 2000 MW or more" should also be better defined. Is it total generation capacity greater than 2000 MW. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Center" to "Each primary Control Center and any backup Control Center" In addition - there is no consideration for generation with a common control system or cyber asset that may span two or more RC foot prints. - there is no consideration for a common cyber system that may control large loads. As well as how the acceptable loss of load threshold for a given area is determined. Could this be an RC responsibility to determine the maximum acceptable load loss? Also the DP should also be considered in the applicability section.
AESI	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
IESO	5. Although Adequate Level of Reliability #5 (ability to restore the system) is included as a critical function, it is limited to blackstart generation and transmission subsystem cranking paths. H and M criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). We would drop 6 generating stations (over 3000 MW) from High (current Critical Assets) to Low using the proposed categorization criteria. There should be a requirement in the High category for generation essential to facilitate restoration as determined by the RC. Item High 1.7 - Exceeding an IROL does not cause instability if recovered within the timeframe allowed by the current standards requirements, and therefore should not be a H or M criterion TLRs are more often used to manage constraints that are binding due to market-market activity. TLRs in and of themselves do not necessarily affect reliability, therefore should not be H or M criteria
Manitoba 2	All comments are prefaced with the section number: 1.3 - Must Run units may only be needed for local area congestion management and therefore should have a Medium BES Impact. All of the High BES Impacts should be prefaced by the question - Do they contribute to instability, separation or cascading? 1.4 - A blackstart plant is not typically critical because there are alternatives available in most blackstart plans. Blackstart plants should be in the Medium BES Impact category unless their size includes them in section 1.1 or 1.2. 1.5 - A 300 kV or higher substation may or may not be critical. If the station loss lead to instability, separation or cascading, then it has a High BES Impact, which is already addresses in sections 1.10 to 1.12. 1.6 - There are typically alternative Cranking Paths. Transmission Subsystems comprising the Cranking Paths should be a Medium BES Impact. 1.13 – These systems shouldn't have an Adverse Reliability Impact. This criteria should instead refer to instability, separation or cascading. 2.2 – This criterion should be qualified as having an Adverse Reliability Impact. 2.5 – A lower bound is required for this criterion, and should be revised to "Each Protection System, Special Protection System, or Remedial Action Scheme Subsystem operated at less than 300 kV and at 100 kV or more in the Eastern and Western Interconnections,

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	or less than 200 kV and at 100 kV or more in other Interconnections that have an Adverse Reliability Impact". 2.6 – "Not included above" should be revised to "not already included in Section 1 above." 3.0 - By the definition, these BES Subsystems do not have an impact on the reliability of the BES, and therefore should belong in a "No BES Impact" category. If a No BES Impact category is not provided, the controls for the Low BES Impact category should not be auditable.
ATC	Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (ATC Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entities are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit. 1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: ATC removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? As a Transmission only company ATC would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	generation) ATC believes strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments on the SDT Attachment 1 document: 1.7 A TLR is a tool used by entities to help control system limits in both a pre-contingency or post-contingency event. We disagree with the SDT assumption that an IROL is equal to a TLR event and therefore should both be identified as high. We recommend that this language be removed from Appendix 1. (NOTE: TLR's are only issued in the Eastern Interconnection.) 1.10 - .12 ATC believes that these should be deleted because they do not fall into the goal of Attachment 1. The goal of Attachment 1 is to provide greater clarity around what BES Facilities should be categorized as either High or Medium. The way these items are written it would force all registered entities to study all of its Transmission Subsystem and show that they do not cause cascading, instability or separation. The other options for the SDT (one we don't recommend) would be to delete items 1.1 – 1.9 because 1.10 and 1.12 requires us to perform engineering assessments.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
IMPA	In 1.12., 2.3, it does not state how an entity is to come to the conclusion of a complete operational failure or cascading outages. It should say as determined through an engineering analysis or other assessment method. In 1.13, 2.5, it does not state how an entity is to come to the conclusion of an item having an Adverse Reliability Impact. IMPA recommends adding as determined through an engineering analysis or other assessment. IMPA would like to see the addition of an impact category for BES Subsystems that have an extremely minimal impact on the BES, and do not get assigned a high percent (70 or 80 percent) of the security requirements for a High or Medium BES Impact asset.
ERCOT	ERCOT ISO supports Midwest ISO Comments. To further improve the proposed criteria, ERCOT ISO recommends that the criteria be based on time frame as well as impact to the BES. Midwest ISO Comments: 1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a "Must Run" unit to add the following phrase at the end of the sentence: "...that have wide area reliability impacts." 3. Add an Item in Category 2 that corresponds to Item 1.3 for "Must run" units that have "local area reliability impacts." 4. In Item 2.6., the word "controlling" needs to be clarified. This item should only encompass Control Centers and back up Control Centers that "remotely control and solely monitor the status of assets" rather than just performing redundant monitoring of those assets. ISO-NE Comments: The Standard should not reference the role of a Reliability Coordinator or Reliability Assurer reviewing a Responsible Entity's "engineering evaluation or other assessment method ". 1. Requirement 1.2 anticipates a so-called "Reliability Assurer" as playing a role in the determination of which BES Subsystems contain Cyber Systems that may be subject to required cyber-security/critical infrastructure protections. 2. If the SDT, in fact, intended for a Reliability Coordinator or Reliability Assurer to have an obligation to review and ultimately approve Responsible Entity's evaluations/methods, such a Requirement would be contrary to Order Nos. 706 & 706-A. By including in a Reliability Standard that a Reliability Coordinator may approve evaluations/methods, the Standard Drafting Team appears to place ultimate responsibility on the designation of assets as requiring critical infrastructure protections on the Reliability Coordinator. Order No. 706A reaffirmed that a Responsible Entity must be solely responsible for identifying those assets that are subject to critical infrastructure protections. In Paragraph 53 of 706-A, FERC stated that: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity
PacifiCorp	Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. PacifiCorp submits that the security controls work must be completed to determine what categorizations are possible and needed.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	PacifiCorp has reviewed the existing controls and observes the following: many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, PacifiCorp recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) in question 13, but moving the categorization aspects of CIP-002-4 into the development work with security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might on the list as one, but not the only, acceptable method to achieve the objective of low electronic authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, PacifiCorp submits that the development of Attachment 1's concepts be concurrent with the security controls work. If the security controls developed support the need for categorizations based on concepts in Attachment 1, the attachment should strive to eliminate the need for creating new definitions and concepts for these subsystems. Attachment 1 is hindered by the issues identified with the confusing definitions for Generation Subsystem and Transmission subsystem. Where meaningful categorizations are identified, their criteria should be bright line. PacifiCorp recommends bright lines that do not necessitate engineering analyses or third party review. A bright line approach will ensure consistent, standardized, and auditable requirements. Further, a bright line approach, if designed properly, will be an effective and efficient way to protect the BES from a concerted well-planned cyber attack. Specifically, PacifiCorp suggests the following to improve the specific criteria currently listed in Attachment 1: • Section 1.4, 1.6: PacifiCorp suggests that the Cranking Path requirement be further defined. Many utilities have designated many potential cranking paths, some which are considered primary or preferred paths while others are alternative paths. PacifiCorp suggests establishing a megawatt level criteria in order to properly categorize the impact to the BES of different blackstart units

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	and Cranking Paths. For instance, small generating units under a certain megawatt nameplate could be excluded unless the unit is in the primary black start path because the other small units have minimal risk of contributing to success of a concerted, well-planned attack against multiple points. • Section 1.5: PacifiCorp suggests that the specific number of lines coming from a substation should not be a consideration. Rather, the specific nature of the lines i.e. station duty, fault duty and flow levels, should be considered. • Section 1.13: The reference to SPS or RAS Subsystem is unclear. PacifiCorp would currently consider its SPS to be a cyber system, housed within a critical substation. PacifiCorp suggests that SPS Subsystem should be defined separately.
PEPCO	Proposed amendments to Attachment 1 were provided earlier.
NEI	A) Suggest rewording 1.2 to strike reference to contingency reserve or total reserve sharing obligations. The wording is suggested to be "Any critical generating unit or plant." B) The functional approach for determining impact categories would provide the opportunity to clearly define what is most important and what needs the greatest attention. It's important to recognize that most any system is designed to continue to operate successfully, even under conditions where some parts are not optimally functioning. The factor of how long can you continue with without certain components helps to prioritize the protection necessary. Also, many systems contain algorithms to address fault conditions and back-up components for failed occurrences. These factors don't seem to come into consideration under the current draft standard approach. C) Apply them appropriately. Hierarchical categorization of loss impact of individual electric operating sites/assets may be useful in defining physical security standards. But electric grid asset rating/size categorization is not salient to definition of hierarchical security controls and countermeasures requirements for cyber assets. Hierarchical sets of requirements (controls and countermeasures) are needed for cyber assets themselves, based upon how much risk they themselves pose to reliable operation of the bulk electric system should they be lost or compromised. D) In general we disagree with the H/M/L classification driven by Attachment 1, and in particular some of the classifications between H/M seem arbitrary, especially the size of generation subsystems. We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. E) As presented, we believe Attachment 1 could be improved by eliminating 1.10, 1.11 and 1.12 which are redundant with 1.7.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

Summary Consideration: LSE

Organization	Question 9 Comments for LSE (Response page 21)
GSOC/OPC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Consumers	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
MPPA	MPPA has concern expanding the applicability to Load-Serving Entities. Any BES assets a LSE may have should be sufficiently covered by the attachments. Adding LSE's does not add value or increase the reliability of the BES.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since LSEs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.

Organization	Question 9 Comments for LSE (Response page 21)
Calpine	Suggested Criteria for load serving entities Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
Flathead	Eliminate Low BES Impact assets as by definition they are not critical.
Carthage	Can this function impact the BES in real time? If so, please explain how. Should this function automatically be placed in the Low BES Impact category? If not please explain why.
Entergy	Use of “routable protocols” is the bright line sought, regardless of electric asset size/rating/type. See Entergy’s response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Load Serving Entities: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	Load Serving Entities should have applicability to the standard only if they operate transmission protection equipment or Special Protection Systems (SPS)
O&R	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
Alliant	We believe they should not fall under the applicability of this Standard.

Organization	Question 9 Comments for LSE (Response page 21)
Ameren	From a System perspective, loss of load should be commensurate with the loss of generation. This would be applicable to LSE
Black Hills	Not at this time.
NVEnergy	None; these entities do not generally impact the reliable operation of the BES.
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	Given that a LSE that owns assets used to serve customer load is also a Distribution Provider, we do not see any reason to include the LSE function in the applicability of this standard (include the DP)
BPA Trans	none
KCPL	No comments
MidAmerican	The characteristics and connectivity of their Cyber Assets will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
CPG	No comment
Santee Cooper	no
Oncor	We question whether they should even fall under the applicability of this Standard.
NGRID	National Grid does not have any suggested criteria for LSE, TSP, or IC.
MGE	LSEs should be removed from the applicability section of this Standard.
FE	"Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS.
TECO	We support EEI's comments on this item.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.

Organization	Question 9 Comments for LSE (Response page 21)
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
Allegheny power	AP proposes following the example of the amended Attachment 1, namely: • Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have a material adverse reliability impact, • Subsystems that perform automatic load shedding of 300 MW or more.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any LSE Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.
AESI	none
ATC	LSEs should be removed from the applicability section of this Standard. LSEs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please

<table>
<tr><th>Organization</th><th>Question 9 Comments for LSE (Response page 21)</th></tr>
<tr><td></td><td>contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.</td></tr>
<tr><td>IMPA</td><td>none</td></tr>
<tr><td>PacifiCorp</td><td>Suggested Criteria for Load Serving Entities: The standard should apply to Load-Serving Entities if they operate transmission protection equipment or a Special Protection System (SPS).</td></tr>
<tr><td>PEPCO</td><td>Load Serving Entities should have applicability to the standard only if they operate transmission protection equipment or Special Protection Systems (SPS)</td></tr>
</table>

Summary Consideration: **TSP**

Organization	Question 9 Comments for TSP (Response page 21)
GSOC/OPC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since TSPs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Carthage	No comments
Entergy	Use of "routable protocols" is the bright line sought, regardless of electric asset size/rating/type. See Entergy's response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Transmission Service Providers: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	TPSs should be removed from the applicability section of this Standard. TPSs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems.

Organization	Question 9 Comments for TSP (Response page 21)
Alliant	We believe they should not fall under the applicability of this Standard.
Black Hills	Not at this time.
NVEnergy	None; the requirements applied to the Transmission Owner/Operator are sufficient.
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	none
BPA Trans	none
KCPL	No comments
MidAmerican	TSPs do not have cyber assets.
CPG	No comment
Santee Cooper	no
Oncor	We question whether they should even fall under the applicability of this Standard.
MGE	TSPs should be removed from the applicability section of this Standard.
FE	TSP facilities interact with the BES like a control center. Therefore, TSP Cyber Systems should be categorized as like a Control Center.
TECO	We support EEI's comments on this item. However, we note that EEI may have used the acronym TPS instead of TSP.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.

Organization	Question 9 Comments for TSP (Response page 21)
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any TSP Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.
AESI	none
ATC	TPSs should be removed from the applicability section of this Standard. TPSs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems.
PSE	It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.
IMPA	none
PacifiCorp	Suggested Criteria for Transmission Service Providers: The standard should not be applicable to Transmission Service Providers because Transmission Service Providers to not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type. • High = data/control/operations/system administration centers using TCP/IP networking; • Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.

Summary Consideration: IC

Organization	Question 9 Comments for IC (Response page 21)
GSOC/OPC	none
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since ICs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Carthage	No comments
Entergy	Use of "routable protocols" is the bright line sought, regardless of electric asset size/rating/type. See Entergy's response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Interchange Coordinators: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	EEI proposes following the example of the amended Attachment 1, namely, only those entities that operate: • Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern

Organization	Question 9 Comments for IC (Response page 21)
	and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have a material adverse reliability impact, • Subsystems that perform automatic load shedding of 300 MW or more.
Alliant	We believe they should not fall under the applicability of this Standard.
Black Hills	Not at this time.
NVEnergy	No criteria are necessary; interchange coordinator does not have the capacity to affect the security of the BES.
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	none
BPA Trans	none
KCPL	No comments
MidAmerican	This is not a defined entity in the NERC Glossary.
CPG	No comment
Santee Cooper	no
OGE	• Should these entities be included? • Can they impact the BES in real time? • Do they automatically go to Low BES Impact?
MGE	ICs should be removed from the applicability section of this Standard.
Teco	None
MRO	We feel they should not fall under the applicability of this Standard.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.

Organization	Question 9 Comments for IC (Response page 21)
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any Interchange Coordinator Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.
AESI	None We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
ATC	ICs should be removed from the applicability section of this Standard. ICs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems. Lastly, ATC does not have any suggested criteria for LSE, TSP or IC, but believes that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
PSE	It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.
IMPA	none
PacifiCorp	Suggested Criteria for Interchange Coordinators: Interchange Coordinator is not a term defined in the NERC Glossary. See response to question 8 for all three of the above. The characteristics and connectivity of their Cyber Assets will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type. • High = data/control/operations/system administration centers using TCP/IP networking; • Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type.

Organization	Question 9 Comments for IC (Response page 21)
	• High = data/control/operations/system administration centers using TCP/IP networking; • Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

Summary Consideration:

Organization	Question 10 Comments (Response page 22)
GSOC/OPC	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
Consumers	Comment #1: We believe that NERC and Regional Entities should have to identify those Cyber Systems that contain industry sensitive information. (Examples: Associated with TFE requests or Sensitive National Security Information) Comment #2: We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
NPCC	Recommend that the SDT review the impact of NERCnet and Cyber Systems connected to NERCnet.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. These entities do not own the assets in question, so they should be removed from the applicability section. Unless of course the SDT takes our suggestion above under Q7. If so, all other registered entity types but NERC and the REs should be removed.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: We believe that NERC and Regional Entities should have to identify those Cyber Systems that contain industry sensitive information. (Examples: Associated with TFE requests or Sensitive National Security Information) Comment #2: We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
SOCO	Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for

Organization	Question 10 Comments (Response page 22)
	equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009, or a category for minimal-risk or no-risk subsystems must be created.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Edison Mission	1. Although it is not known to us at this point what controls or levels of protection would be required for the 3 suggested levels of High, Medium or Low impact. I would like to suggest that there also be a fourth category of No Impact. It would seem to me that there are more than a few generating facilities that would have no impact on the reliability of the BES be it a small generating station or wind facility. 2. In CIP-002-4 under Attachment 1 under High Impact (1.4) it states that "Each Blackstart Generation Subsystem that has been included in the regional Blackstart capability plan" Some Blackstart units included in the Blackstart capability plan are not necessarily critical to restoration of the BES if there were a power outage.
Calpine	Suggested Criteria for load serving entities Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
Flathead	Eliminate low impact.
Carthage	No comments
Entergy	See Comments under Question 13; most likely “High”

Organization	Question 10 Comments (Response page 22)
CenterPoint	Suggested criteria for NERC and Regional Entities: None at this time. It is not clear criteria needs to be developed for these entities.
NIPSCO	We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.. Suggestion: Review the intended scope of the term control center and clarify the intent with revised or additional language.
ConEd	The criteria should be simplified and having 3 levels makes determining which one applies very difficult and confusing.
EEI	NERC and the Regional Entities can voluntarily adopt these requirements if they believe that the requirements are necessary for their organization. NERC also has the option to require all or certain requirements to the Regional Entity through the Delegation Agreement.
O&R	Please refer to question 8. The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
Alliant	We believe they should not fall under the applicability of this Standard.
Ameren	We see no role for NERC or Regional Entities in this regard as these entities should make sure that they have nothing that is capable of impacting the operation of the BES.
Black Hills	Not at this time.
NVEnergy	None; NERC and Regional Entities do not own or operate BES facilities, and therefore no criteria would apply.
MWDSC	Recommend creating a separate category for "No BES Impact". Criteria would be to demonstrate no Adverse Reliability Impact using an engineering evaluation.
Empire	These entities should be outside of the scope of this standard.
SCEG	If NERC/Regional Entities are considering collecting/retaining any information pertaining to CIP-002-4 from entities, any systems responsible for housing/managing/retaining such information should be considered a high impact category.
Exelon	No opinion at this time.
BPA Trans	Suggested criteria for NERC and Regional Entities: The criterion needs to be simple and clear. Criteria such and MW generation or load served by a transmission system is good. Criteria that requires studying loss of equipment beyond that done for normal planning creates additional workload with little benefit.
HQT	Recommend that the SDT review the impact of NERCnet and Cyber Systems connected to NERCnet

Organization	Question 10 Comments (Response page 22)
Allegheny Energy	We are concerned that due to the potential scope of the proposed CIP-002 version 4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
KCPL	No comments
MidAmerican	See response to question 8 and 9. The characteristics and connectivity of their Cyber Assets, if any, will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
CPG	No comment
Santee Cooper	no
OGE	• Should these entities be included? • Can they impact the BES in real time? • Do they automatically go to Low BES Impact?
NGRID	It is not clear as to why the SDT is including NERC and Regional Entities in the applicability of this standard. NERC and Regional Entities are not subject to the Compliance and Enforcement Program and therefore having them list in the applicability section only confuses the issue of who has to comply with this standard.
MGE	They should be removed; neither has any impact on the real time reliability of the BES and are not users, owners or operators of the BES.
TECO	We support EEI's comments on this item.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.

Organization	Question 10 Comments (Response page 22)
Duke	Any NERC or Regional Entity Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact, and protected accordingly.
AESI	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
ATC	ATC does not understand why the SDT is including NERC and Regional Entities in the applicability of this standard. NERC and Regional Entities are not subject to the Compliance and Enforcement Program and therefore having them list in the applicability section only confuses the issue of who has to comply with this standard. NERC and the Regional Entities can voluntarily adopt these requirements if they believe that the requirements are necessary for there organization. NERC also has the option to require all or certain requirements to the Regional Entity through the Delegation Agreement. We believe that these two entities should be deleted from the Applicability Section.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable –	✓						

<table>
<tr><th>Organization</th><th>Question 10 Comments (Response page 22)</th></tr>
<tr><td></td><td>
<table>
<tr><td>Private</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>IMPA</td><td>none</td></tr>
<tr><td>ERCOT</td><td>The functions of NERC and the Regional Entities do not lend them to alignment with the CIP standards. However, the information they possess could have a severe, if indirect, long term impact on the BES if not properly protected. With this in mind, it may be necessary to draft additional guidance for NERC and the Regional Entities regarding information protection. This would provide adequate instruction to NERC and the Regional Entities as well as provide a level of understanding and assurance for other Responsible Entities.</td></tr>
<tr><td>NEI</td><td>A) Clarify that the purpose of the question is to differentiate between the criteria for LSE, TSP and IC and the criteria for NERC and ROs.
B) If yes, then see #9 – no different; most likely “High”</td></tr>
</table>

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?

Summary Consideration: DP

Organization	Question 11 Comments for DP (Response page 23)
Progress Energy	The DP should be added if it has cyber systems that could access and impact the reliability of the BES and/or if the DP owns cyber systems that are shared with Transmission subsystems.
GSOC/OPC	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Hayden	If NERC continues to use the definition of BES as 100 kv or higher then a Distribution provider would not be under this jurisdiction. Alternatively, what if a Distribution Provider can load shed >300 MW of power? Are they now included? These are very key considerations -- especially with the new use of smart meters/smart grid technology.
SDGE	In general, we feel that the CIP Standards should not be applicable to the Distribution System or Distribution Providers. The transmission system benefits the most from the requirements in the CIP Standards.
APPA	The APPA Task Force recommends substituting DP for current applicability to LSEs. LSEs do not own BES facilities. The DP may own certain very limited BES assets, generally limited to UFLS and UVLS relays. Associated BES Cyber Systems used to control the operation of these relays or transmit relay operations data to higher level entities (generally, the Transmission Operator) may properly be subject to BES classification under proposed CIP-002-4.
Consumers	Comment #1: We do not have any suggested criteria for DP or RA, but believe that if the SDT is unable to identify any specific criteria then these two entities should be removed from the standard. Comment #2: We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10
NPCC	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.
MPPA	MPPA has concern expanding the applicability to Distribution Provider's. Any BES asset a DP may have should be sufficiently covered by the attachments. Adding DP's will not add value or increase the reliability of the BES.

Organization	Question 11 Comments for DP (Response page 23)
Central Lincoln	While DPs own electrical assets, those assets are not considered to be within the BES. They should not be included.
NERC	Distribution Providers should be included on the list to acknowledge their support for load shedding functions. While directed by the Transmission Operator, oftentimes, the Distribution Provider is the practical implementer of the request and may have Cyber Systems that support this important BES activity.
Dominion	Do not add “Distribution Provider” to the list. By definition, Distribution is not part of the BES.
Dyonyx	Inclusion of Distribution Providers does not appear to be applicable to the intent of this Standard.
Oregon PUC	No comment
Manitoba 1	depends on the affect I assume on the BES.
Portland GE	No comment at this time
PSEG	Comment #1: We do not have any suggested criteria for DP or RA, but believe that if the SDT is unable to identify any specific criteria then these two entities should be removed from the standard. Comment #2: We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES.
WE-Energies	Wisconsin Electric Power Company agrees with EEI’s suggestions regarding this question.
Idaho Power	Not appropriate to include. Minimal to no impact on the BES. Expands the scope beyond the BES.
SOCO	The DP function should not be added to the CIP standards at all.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Calpine	Doesn't appear to affect the functionality of the BES
Flathead	Opposed. This regulatory scheme was not intended to regulate local distribution, but continues to do so beyond FERC intent or authority. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at LSE/DPs that didn't identify critical assets.
E ON	Distribution is usually 69 kV and below, which is not BES (>100kV). Hence, they should not be added. Moreover, Section 215 (a)(1) provides that facilities used for distributing electric energy do not comprise part of the bulk power system. Sections 215(a)(2) & 215(a)(3) provide that the ERO and standards developed by the ERO address the Bulk Power System only. Cyber systems that are associated with both distribution facilities and BES subsystems should, by virtue of being associated with BES subsystem, already fall under the

Organization	Question 11 Comments for DP (Response page 23)
	requirements of the standard. There is no need to include cyber systems associated solely with distribution facilities.
Carthage	Can this function impact the BES in real time? If so, please explain how.
Entergy	If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see Comments under Question 13.
CenterPoint	CenterPoint Energy does not agree with expanding applicability of this standard purporting to address Bulk Electric Reliability to Distribution Providers. The functions assigned to Distribution Providers by the NERC Standards are generally limited to load shedding functions, which are addressed by the currently CIP-002 standard through consideration of assets that shed 300 MW or more through a common system.
NIPSCO	We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10. We do not have any suggested criteria for DP, but believe that if the SDT is unable to identify any specific criteria then this entity should be removed from the standard.
ConEd	Yes, the standard should apply to the extent that UFLS or UVLS programs are under the control of the DP.
EEI	Distribution Providers should have applicability to the standard only if they operate transmission protection equipment or Special Protection System (SPS)
Alliant	We believe this Standard should only apply to Distribution Providers that own/operate BES assets
Ameren	SDT should provide reasons to include these entities as we have not seen any evidence to include these entities.
Black Hills	Should not be included.
NVEnergy	There is no reliability justification to include distribution providers as applicable entities.
SWTC	Will this require a entities to register as a Distribution Provider if they are not in the NERC Registry?
SCEG	none
Exelon	Exelon believes that the DP function should be added and LSE function should be eliminated from this standard applicability.
BPA Trans	None
HQT	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.

Organization	Question 11 Comments for DP (Response page 23)
KCPL	Depending on the criteria established, it is a possibility.
MidAmerican	Standards should be applicable to distribution providers and load serving entities if they own BES assets that meet the criteria for the BES as defined by NERC.
CPG	No comment
Santee Cooper	Would only include a DP if they own facilities that would cause BES outages.
OGE	• Inclusion of the Distribution Provider would require a significant lead time, resources and financial investment. • What authority does a Reliability Assurer have to regulate a distribution provider?
Oncor	We feel this Standard should only apply to Distribution Providers that own/operate BES assets.
NGRID	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.
MGE	Only if the DP own BES assets under the definition of what a Distribution Provider is. If the DP did own or operate BES assets, wouldn't they be registered as a TO or TOP?
FE	"Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS.
TECO	We do not support the addition of DP.
CECD	Should not be included.
MRO	We feel this Standard should only apply to Distribution Providers that own/operate BES assets.
GTC	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Xcel	We feel this Standard should only apply to Distribution Providers that own/operate BES assets
BGE	We believe that Distribution Provider should not be included at this time as an applicable entity for this standard.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	We feel that expanding it to any facility is not necessary as this does not meet the definition of the BES.

Organization	Question 11 Comments for DP (Response page 23)
TAPS	See TAPS response to Question 1.a.
Allegheny Power	Distribution Provider and Load Serving Entities should have applicability to the standard if they operate transmission protection equipment or Special Protection System (SPS).
FMPA	DPs are probably more important to include than LSEs. LSEs usually do not control breakers for instance, where DPs often do. The same criteria should be used for all Entities because the bottom line is avoiding “instability, uncontrolled separation, and cascading”, which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	They should be included if they have a Cyber System that could be exploited to impact BES reliability.
NBSO	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added. DP's with a common control system or Cyber Asset that can impact a significant amount of load may not be captured in the registration process yet have impact.
AESI	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Manitoba 2	Due to the potential impact that centralized control of a large number of distribution assets could have on the reliability of the BES, Distribution Providers should be considered within the scope of these standards.
OMPA	All Distribution Providers or only those that own and operate BES assets?
ATC	Do not add the Distribution Provider because entities with this registration have responsibility for distribution systems, rather than the BES. If an entity has responsibility for the BES reliable operation, then they would be registered as a Transmission Owner or Transmission Operator.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

<table>
<tr><th>Organization</th><th>Question 11 Comments for DP (Response page 23)</th></tr>
<tr><td></td><td>
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Only if they own SPS.</td></tr>
<tr><td>IMPA</td><td>IMPA does not believe that a Distribution Provider should be added unless an engineering analysis shows that it has an Adverse Reliability Impact on the BES.</td></tr>
</table>

Organization	Question 11 Comments for DP (Response page 23)
PacifiCorp	Comments on adding Distribution Provider: The standard should apply to Distribution Provider and if they operate transmission protection equipment or a Special Protection System (SPS).
PEPCO	Distribution Providers should have applicability to the standard only if they operate transmission protection equipment or Special Protection System (SPS)
NEI	Some believe DP should have applicability, some believe they should not. "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. However, when considered, if their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see #9.

Summary Consideration: **RA**

Organization	Question 11 Comments for RA (Response page 23)
Progress Energy	NERC needs to define Reliability Assurer.
GSOC/OPC	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Consumers	Comment #3: We do not believe that DP adds value. RA may add value in regards to information protection / information assurance.
NPCC	Recommend that Reliability Assurer not be added to the list of applicable Functional Entities. NPCC does not provide real time operational input.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. These entities do not own the assets in question, so they should not be included.
Dominion	Add “Reliability Assurer” to the list. Since Attachment 1 requires an “engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer” there should be a requirement imposed on these entities to develop criteria for each. See comment to item 4 above.
USBR	Reliability Assurer is only defined in the Reliability Functional Model and is not included as a defined term in the Glossary of Standards. This treatment is inconsistent with the other functions. The term will need to be defined in order to be used in the Reliability Standards. It is not cleat that the role is needed in this standard.
Green Country	Who, what, when, where, why and how....?? Never heard of this function
Oregon PUC	No comment
Manitoba 1	No comments
Portland GE	No comment at this time
PSEG	Adding the RA functional entity type would be as described in question #10. Comment #3: We do not believe that DP adds value. RA may add value in regards to information protection / information assurance.
WE-Energies	Wisconsin Electric Power Company agrees with EEI’s suggestions regarding this question.
Idaho Power	Need a definition of what this function is. This would seem to be a responsibility of all the registered entities.
SOCO	Currently we don’t know who this is. Not being defined in any approved functional model.

Organization	Question 11 Comments for RA (Response page 23)
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional role is not yet approved or in effect.
Calpine	The definition of Reliability Assurer is unclear to us.
Flathead	This should be Regional Reliability Organization or Reliability Coordinator.
E ON	It is unclear to E ON U.S. what this term means. “Reliability Assurer” is not in the NERC Glossary of Terms neither is it defined in this draft standard. E ON US objects to the inclusion of this term.
Carthage	No comments
Entergy	If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see Comments under Question 13.
CenterPoint	The term of Reliability Assurer needs to be defined.
NIPSCO	We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10. We do not have any suggested criteria for RA, but believe that if the SDT is unable to identify any specific criteria then this entity should be removed from the standard.
ConEd	Yes, since the Reliability Assurer has a role in reviewing and approving models and engineering studies.
Alliant	Reliability Assurer needs to be adequately defined before we can make a judgment on this.
Black Hills	RA's should be included.
NVEnergy	The functions of a Reliability Assurer do not include the ownership or direct operation of BES facilities; therefore this standard should not be applicable
NCEMCS	Given the high probability that DP facilities would all fall under the low impact category, this inclusion would do very little to benefit the reliable operation of the BES but would add significant cost to distribution co-operatives and ultimately their end user members.
SCEG	none
Exelon	No comment
BPA Trans	None

Organization	Question 11 Comments for RA (Response page 23)
HQT	Recommend that Reliability Assurer should not be added to the list of applicable Functional Entities. NPCC does not provide real time operational input.
KCPL	No comments
MidAmerican	Reliability Assurer is not in the NERC Glossary of Terms. MidAmerican's proposed changes to CIP-002-2 eliminate the need for a reference to Reliability Assurer.
CPG	No comment
Santee Cooper	none
NGRID	National Grid recommends that Reliability Assurer should not be added to the list of applicable Functional Entities.
MGE	This is undefined, the question cannot be answered.
TECO	It is not clear to us what BES subsystems would apply to an RA, therefore we cannot make a determination on this.
CECD	Should be included.
MRO	This is difficult to ascertain without knowing the formal definition of a Reliability Assurer. We feel these needs to be defined in the NERC Glossary of Terms.
GTC	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Xcel	This is difficult to ascertain without knowing the formal definition of a Reliability Assurer. We feel these needs to be defined in the NERC Glossary of Terms.
BGE	This term should be included in the "NERC Glossary of Terms used in Reliability Standards."
FPL	This function is not yet FERC approved. See previous comments on this matter.
TAPS	See TAPS response to Question 1.a.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs. It is unlikely that the RA will have any such Cyber Systems.
Duke	They should be included if they have a Cyber System that could be exploited to impact BES reliability.
AESI	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be

Organization	Question 11 Comments for RA (Response page 23)
	adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Manitoba 2	We are unfamiliar with the term “Reliability Assurer” and are unable to comment.
OMPA	Cannot comment; unsure of the definition of “Reliability Assurer”.
ATC	Do not add the Reliability Assurer because we understand these entities to have responsibility for monitoring compliance with the reliability standards requirements. So, they should be accountable for requirements that they are responsible for monitoring (e.g. conflict of interest). In addition, we understand that registration for the Reliability Assurer has not been established yet.
IMPA	IMPA might see where this entity could be added to ensure approvals of engineering evaluations or other assessment methods are performed in a timely manner and equally across the region or the country.
ERCOT	ERCOT ISO reads the applicable Function Entities list to not include the “Reliability Assurer”. Further, there is ambiguity as to what organizations would be registered as a Reliability Assurer. This is an active discussion item with the Functional Model Working Group.
PacifiCorp	Comments on adding Reliability Assurer: Reliability Assurer is not a term defined in the NERC Glossary of Terms.
NEI	This functional role is not yet approved nor in effect. When the role is approved and in effect, CIP 002-4 should apply (note that they have a function for performing or reviewing Engineered Evaluation already). If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see #9.

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

Summary Consideration:

Organization	Question 12 Comments (Response page 24)
Progress Energy	Tools that are used in the planning horizon are not critical to BES reliability and should be removed from the proposed functions. (e.g. Unit Commitment under Balancing Load and Generation.) The focus for these proposed functions should be cyber systems that support real-time operations.
GSOC/OPC	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems might have on the BES and subsequently the impact which should be assigned to them.
Hayden	In the July 21, 2009 NERC Concept Paper "Categorizing Cyber Systems An Approach Based on BES Reliability Functions," there is a list of BES functions that is not identical to the list in CIP-002-4 Attachment 2. As a suggestion for consistency and to take advantage of the thoroughness of the info in the Concept Paper, why not use the nine functions identified in Figure 1 and Table 1 which include: 1) Contingency Reserve/Peakers; 2) Load Balancing, Frequency Response/Support; 3) Voltage Support/Reactive Power Supply; 4) Constraint Management; 5) Control and Operation; 6) Situation Awareness; 7) Restoration; 8) System Stability; 9) Load Management
Consumers	Attachment 2 is a listing of high-level tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
NPCC	Please clarify “control” in 6 – Control & Operation. Recommend adding parameterization, calibration to 6 – Control & Operation. Suggest that the words for 8 - Situational Awareness should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing from “The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions.” to “The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES.” Recommend changing 9- Inter-Entity Coordination and Communication from “The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.” to “only inter-utility data communications”. Existing language would include voice communications. Attachment 2 is not careful as to whether it applies only to BES Elements. If it is taken to apply to any Element then it becomes a definition of the BES System.

Organization	Question 12 Comments (Response page 24)
Central Lincoln	Make the list complete. The “include, but are not limited to” open ended function list leaves too much room for disagreement.
Dominion	Dominion has the following suggestions: 1. Dynamic Response – Dominion disagrees with the inclusion of Spinning Reserve and Governor Response as neither of these is dependent upon a cyber system. 2. Balancing Load and Generation – Dominion disagrees that any of the listed activities is solely dependent upon a cyber system. These functions can be performed without employing a cyber system. The listed activities should only be included if they are solely dependent on computer systems, intranet or internet to allow access to multiple parties. 3. Restoration of BES – Dominion disagrees with including this function, as most restoration plans assume the transmission operator’s system has suffered a total blackout. It is extremely doubtful in this case that any cyber systems will be used, because each step of the process will have to be manually tracked. Inclusion should be determined on a case-by-case basis based upon the specific restoration plan.
Encari	We recommend reviewing for inclusion the following critical functions: 1. Emission systems (with indirect impacts) 2. Remote Cyber Support
USBR	Dynamic Response Section Spinning Reserve is listed which by itself is not an automatically triggered and not a Dynamic Response quantity. Units, or capacity so designated, is controlled by AGC. Governor Response should specifically mention AGC. Unless its control is addressable, Governor frequency response should not be included as a part of the Cyber standard. Excitation Systems with Automatic Voltage Regulators are not listed and should be. Under and Over Frequency Relay, Under and Over Voltage Relays are covered under Protection Systems. To call them out separately implies otherwise. AGC should not be listed in the Controlling Frequency section as it is a Dynamic Response. This Controlling Voltage section does not list "Transmit adjustments to individual units" (in response to a voltage schedule). The Control & Operation section needs to include Generator controls for AVR, and AGC. The Situational Awareness section is covered by the other sections and is not needed.
Westar	Attachment 2 only adds confusion and should be eliminated.
Green Country	Clearly identify if for each function if you need all of the elements below it or just one, to be considered having that function. For example if all you have is power system stabilizers, do you have the Dynamic Response function?

Organization	Question 12 Comments (Response page 24)
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: Attachment 2 is a listing of high-level tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
WE-Energies	In general, there's a mix of prescriptive and non-prescriptive items under each of the categories (include but are not limited to ...). The definition of dynamic response is confusing. Wisconsin Electric Power Company recommends combining 2, Balancing Load and Generation and 3, Controlling Frequency into one category.
Idaho Power	Attachment 2 supports the identification of cyber systems that support critical BES functions but seems to suggest by the title of the attachment that all functions being critical are also high impact and therefore does not assist with the categorization of assets that could potentially be medium or low impact.
SOCO	There are several places where the proposed standard could have unintended consequences with negative effects on reliability. For example, the requirement that all blackstart units registered as part of the regional reliability plan be classified as high-risk could lead to Entities reducing the number of declared blackstart units; an exemption based on an approved engineering study should be allowed. Under many of the 9 categories of functions (i.e. Dynamic Response, etc.) there is a phrase that states “Aspects of BES Dynamic Response include, but are not limited to:”. We feel that “but are not limited to” is too broad and should be deleted. This Standard attempts to establish requirements for a very broad array of equipment and systems having very different functions and vulnerabilities dependent on the physical installation, usage and method in which they are connected. An example is the use of alarms. Controls Centers tend to have a high number of critical alarms with few low priority alarms, while a Generation Unit could have thousands of alarms with the majority being lower informational type alarms. Some of the alarms within a generating unit are prioritized and used for the indication and alerting of non-operation personnel such engineering or maintenance use. A second area is the physical installation configuration of an area. Generation units are typically in continuously manned and guarded location, transmission facilities may be in non-manned and isolated areas. Control Centers are located in a smaller, office type environment, which is more readily enclosed in “six wall” confines. Consideration should be given to moving Attachment 2 to a FAQ document divided into sections discussing the following areas: • Control Centers • Generation Units • Transmission Facilities Attachment 2 1. Dynamic Response - Generator governor controls may be purely mechanical or local electronic controls without connections to remotely accessible systems.

Organization	Question 12 Comments (Response page 24)
	Attachment 2 2. Balancing Load and Generation - This section should be clarified to address the balancing of electrical system load vs. electrical system "supply". It could be interpreted to apply to the pure generation unit control aspect. Is "Manually Initiated Load shedding" the area of interest or the ability to identify. If "identify" this is under the scope of Situational Awareness in Item 8. Attachment 2 8 Situational Awareness - A definition or the intent of "Change management" should be included. Is this the management of change as cover in other sister standards? Suggest that Attachment 2 refer back to engineering studies to determine the level of impact these functions have on the BES for categorization.
DTE	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Functional Model or the Definition of Adequate Level of Reliability.
AEP	This is a very good request in that it seeks the increased clarity that we see as needed in the functional descriptions. AEP believes that this standard needs to be segmented into each applicable function and not try to use a "one size fits all" approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.
Flathead	The situational awareness, control and operations, criteria are so broad that they would include small call centers and local distribution entities that don't have a "control center" under current standards, but might under these standards.
E ON	E ON U.S. recommends the team revisit what is a switch from identifying critical assets to identifying critical BES functions and then requiring the as yet undefined requirements of CIP-003-009 V4 be applied to associated assets. Generating units, RTUs, communications lines and the like are all subject to being out of service, forced or scheduled, yet BPS reliability is maintained. Attachment 2 makes no allowance for system diversity and redundancy Attachment 2 lists monitoring of spinning reserves which requires telemetry from every generating unit. This implies that every generating unit, regardless of size, falls under this standard. This would also seem to include each RTU and all the communication equipment back to the EMS. E ON U.S. has the same concern regarding calculation of ACE. This implies that all communication equipment back from the RTU for every input into the ACE equation. The drafting team should clarify item 5 "Managing Constraints" of Attachment 2. Could this include cyber assets used in the calculation of ATC? Tagging systems used to submit schedules?
Carthage	CWEP feels that Attachment 2 should be eliminated because it causes confusion. CWEP feels that the functions should be specifically covered in Attachment 1 under the impact categories they fit. The way the attachments are designed leaves too much room for interpretation. CWEP is okay with the format of the standard but would like for the criteria to be more specific. Is the bullet under number 1 that deals with under and over frequency relay protection intended for all entities that participate in under or over frequency load shedding or just the bigger entities as stated in Attachment 1 section 1.14? CWEP feels that applicability needs to

Organization	Question 12 Comments (Response page 24)
	be clarified throughout the standard to ensure that it's interpreted correctly. If under or over frequency load shedding are considered critical to the reliability of the BES, it should be clearly defined in the criteria for the impact categories of Attachment 1 what levels of load shedding fit each category like 1.14 of Attachment 1.
WECC	No suggestions, purposed attachment 2 looks comprehensive and well thought out.
Entergy	None
CenterPoint	Function #8 – Situational Awareness is too broad and needs to be better defined. In particular, the "change management" aspect of Situational Awareness is unclear.
LCRA	1. Attachment 2, 8, bullet 2 – Change management should be better defined or removed from the list. 2. Attachment 2, 8, bullet 5 – Frequency monitoring should be better defined so that the loss of a single monitoring point in a many point scheme is not a problem.
NIPSCO	Attachment 2 is a listing of tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating a select subset of the tasks performed by the functional entities seems redundant.
ConEd	Cranking Path should be clearly defined for application in this Standard.
EEI	Replace "Functions Critical to the Reliable Operation" with "Functions that Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances.
O&R	Cranking Path should be clearly defined for application in this Standard.
Alliant	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternate title "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems. Please provide the basis for including each of the items listed.
Ameren	Attachment 2 is overly broad, e.g. managing ATC, situational awareness, etc.
Black Hills	Not at this time.
TNMP	TNMP has concern with creating a definition and then supplementing the definition with an Attachment providing additional criteria and clarification of a term, as addressed with the High BES Impact comments. If a person were to just look in the NERC glossary then they would have no idea there were additional criteria defining a BES Cyber System. If an appendix or attachment is necessary, the definition should clearly reference the additional information. In TNMP's opinion the drafting team needs to review the definition of "BES Cyber System" to ensure the desired clarity and certainty for inclusion and consistency are obtained.

Organization	Question 12 Comments (Response page 24)
NVEnergy	Items 2 and 3 are so closely related that they should be combined (Balancing Load and Generation, Controlling Frequency).
MWDSC	Clarify functions that are critical to reliable operation of interconnected BES, not isolated BES Subsystems.
Empire	If you identify a control center in attachment 2 then this is not needed.
SWTC	THE BES Task Force needs to set the criteria for BES before this Standard can have merit.
SCEG	Suggest adding "Voltage Regulators" to 1. Dynamic Response list.
Exelon	None
BPA Trans	None
HQT	Suggestions for improving proposed functions: Please clarify “control” in 6 – Control & Operation Recommend adding parameterization, calibration to 6 – Control & Operation Suggest that the words for 8 - Situational Awareness should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing from “The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions.” to “The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES.” Recommend changing 9- Inter-Entity Coordination and Communication from “The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.” to “only inter-utility data communications”. Existing language would include voice communications. Attachment 2 has potential for wider application and does not belong in a CIP standard.
Allegheny Energy	Definitions need to be clarified (e.g.): “Governor Response” - is this movement of a governor to respond to frequency deviation? “Providing Actual Reserves” - Are these systems that request additional generation in response to an event?
KCPL	The criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to “plug into” this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
MidAmerican	The nine functions defined in attachment 2 are confusing, too broad and will have different meanings for different entities. It will be difficult to implement and audit using Attachment 2 as proposed. Eliminate attachment 2. Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber

Organization	Question 12 Comments (Response page 24)
	Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. If needed, instead of creating Attachment 2, provide additional bright line specificity for the Cyber Assets expected in existing CIP-002-2 R3.
CPG	The prior version of CIP-002 considered two dimensions of risk. The first dimension of risk considered was impact, which was whether or not a cyber asset was associated with a critical asset. Secondly, it considered vulnerability by determining whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal, the SDT has eliminated any consideration of the risk due to vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest categories of varying degrees of vulnerability (high and low) be added to the criteria in Attachment 2.
Santee Cooper	None
Oncor	Item 8 – Situational Awareness. What does "Change management" mean? Please explain it, or delete.
NGRID	• Replace "Functions Critical to the Reliable Operation" with "Functions that May Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances. • Please clarify "control" in 6 – Control & Operation • Recommend adding parameterization, calibration to 6 – Control & Operation • In 8 - Situational Awareness, suggest these words should be consistent with the real-time operations words for situational awareness in the Control Center definition. • Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES." • Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications"
MGE	Upon review of the Functional Model, there are some items that are contained in Attachment 2 that fall outside of the Functional Model. Please provide the basis of these items. Please clarify that only High and Medium BES Impact items are to be used in Attachment 2, since items listed in the Low BES Impact

Organization	Question 12 Comments (Response page 24)
	category do not have the potential to adversely affect the BES.
TECO	We believe that the list of functions in Attachment 2 is overly broad and will introduce many systems that do not have a direct impact on the reliable operation of the BES subsystems. Please see our previous comments in questions 2 and 6. We are particularly concerned with the Situational Awareness. For example, systems that report on the capability and status of various units for next day planning, if unavailable will not directly impact the reliability of those BES subsystems that they support, and could be easily tracked on a spreadsheet. We are also concerned with Balancing Load and Generation, specifically, the sub heading of Unit commitment. For example, a simple spreadsheet showing the capabilities of generation units (including High, Medium and Low BES Impact Units) that will be used by management for purely informational purposes has no impact on the BES and should not be considered a High Impact BES Cyber System (according to R3.2). Under Situational Awareness: It is unclear whether Change Management applies to IT Systems or change management as it relates to other work being performed on BES subsystems, for example repairs during a unit outage, or replacement of substation equipment. Additional Attachment 2 Questions: “2. Aspects of the Balancing Load and Generation function include, but are not limited to: Load management – Ability to identify load change need – Ability to implement load changes • Demand Response – Ability to identify load change need – Ability to implement load changes “ These functions may be outside the Control Center. It is not clear if the intent would be to expand scope beyond the control center. 5. Managing Constraints “Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.” Is the intent to pull systems such as Oasis and OATT into scope under managing constraints?
MRO	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternative title of “Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems”. We would also appreciate if the Standard Drafting Team could provide the basis for including each of these items.
GTC	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems

Organization	Question 12 Comments (Response page 24)
	might have on the BES and subsequently the impact which should be assigned to them.
Xcel	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternative title of "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems". Flexibility needs to be incorporated into these definitions to allow exclusion of cyber systems that are not critical to the operation of the BES Generation or Transmission Subsystem. Failure or compromise of some cyber systems may not impact the operation of the subsystem for a significant length of time, allowing for repair. These systems should be excluded from the standard. For example, a PC based coal receiving unloading system. The fuel inventory on-site will supply the plant for a number of days, weeks or months depending upon the amount in inventory." No reliability improvement would be gained from applying cyber controls to this system. We would also appreciate if the Standard Drafting Team could provide the basis for including each of these items
BGE	The prior version of CIP-002 considered two dimension of risk. They considered impact, whether or not a cyber asset was associated with a critical asset. And they considered vulnerability, whether a cyber asset was accessible by dial-up or routable protocol, or if it was not. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal the SDT has eliminated any consideration of the dimension of vulnerability from the standard. It is doubtful that the goal of a establishing practical and appropriate controls can be done without it. We would suggest that various categorization of vulnerability be designated in CIP-002 (High, Medium, Low or High, Low, No?) and the sorting criteria be established in an appendix, similar to Attachment 1 that correspondingly deals with the dimension of impact.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
Allegheny power	AP suggests eliminating Attachment 2.
FMPA	FMPA would beg to differ on the wording of the question, Attachment 2 does not contain functions "critical" to the reliable operations of the BES, but rather activities to maintain the reliable operation of the BES. FMPA recommends eliminating Attachment 2 altogether or creating a supporting paper of "things to consider", or at most, a bullet item list in the requirements of the standard of "activities to consider when evaluating worst case scenarios / contingencies that can be caused by malicious use of a cyber system" If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? And the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. Therefore, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is

Organization	Question 12 Comments (Response page 24)
	certainly NOT critical. Calculation of ACE is certainly NOT critical. Etc., Etc. This standard should focus on what is truly critical, threats of an Adverse Reliability Impact of “instability, uncontrolled separation, or cascading”.
Duke	In addition to identifying functions that impact BES reliability, it should also address categorizing the risk associated with different types of Cyber Systems (i.e. systems that are part of a routable protocol control system network have higher risk than those which utilize serial or dial-up communications), etc.
NBSO	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.” to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline
AESI	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems might have on the BES and subsequently the impact which should be assigned to them.
Manitoba 2	The term “functions critical” should be changed to “functions essential”. The functions list is fairly comprehensive.
OMPA	For Item 6: Control & Operation; OMPA suggests the example should include “electronic” control rather than “all” control.
ATC	Replace “Functions Critical to the Reliable Operation” with “Functions that May Affect the Reliability of the Operation”. This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances. Item 8: - Change management - Current Day and Next Day planning What is the team attempting to identify with these items? They both could be interpreted to mean outage scheduling applications.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to

<table>
<tr><th>Organization</th><th>Question 12 Comments (Response page 24)</th></tr>
<tr><td></td><td>remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Will look to review further in the next draft as more specificity is detailed.</td></tr>
<tr><td>IMPA</td><td>IMPA does not believe all of the functions listed in Attachment 2 will always be critical to the reliable operation of the Bulk Electric</td></tr>
</table>

Organization	Question 12 Comments (Response page 24)
	System. The title of the document should be changed to reflect this issue by eliminating the word critical.
ERCOT	In Attachment 2, Section 3 we assume that it was intended to state “but are not limited to”.
PacifiCorp	The nine functions defined in attachment 2 are confusing, too broad and will have different meanings for different entities. It will be difficult to implement and audit using Attachment 2 as proposed. PacifiCorp proposes eliminating Attachment 2 on the basis that the concept of Critical Cyber Asset should be retained as security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a “system.” The qualifying criteria that consider routable protocol or dial-up accessibility should be retained because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. If needed, instead creating Attachment 2, provide additional bright line specificity for the Cyber Assets expected in existing CIP-002-2 R3.
NEI	A) Revise to consider cyber first, then the impact to the BES. B) Dynamic response not considered – Don’t require cyber systems to balance load and generation. C) There is a concern with the matrix of cyber vs. BES: Something with high cyber impact may have no impact on BES and something with high impact on BES may have no cyber impact. This is not a 1:1 relationship, yet it appears to be treated as such. D) This standard needs to be segmented into each applicable function and not try to use a “one size fits all” approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.

13. Do you have any other comments to improve the draft standard?

Summary Consideration:

Organization	Question 13 Comments (Response page 25)
Progress Energy	In Attachment 1, propose removing "1.2 - Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations." Need clarification on why this criterion was chosen as a High BES Impact.
EPSA	The Electric Power Supply Association (EPSA) appreciates the opportunity to comment on Standards Drafting Team's (SDT) revisions to the Critical Infrastructure Protection (CIP) Standard 2, Version 4 regarding Critical Asset Identification for Bulk Electric System (BES) assets for Cyber System Categorization. The BES serves as the essential highway for competitive generators to cost effectively deliver electricity to customers. Moreover, the development of the CIP standards is essential to ensuring grid security and reliability for electricity customers. I. Background and Overview Competitive suppliers recognize the SDT's challenge of balancing traditional societal electricity goals of reliability and reasonable costs with a new goal -- security. EPSA strongly supports the principles that the SDT seeks to achieve by protecting the BES through the prevention of system instability, prevention of critical subsystem separation and ensuring against cascading outages. Therefore, EPSA is providing additional criteria that the SDT should include in the standard to better link the tiered approach with the articulated principles. The electric power industry is the most capital intensive industry in the U.S. Electric generation is the bulk of this investment, representing more than 70 percent of the average consumer's bill. It appears that it is NERC's view that there should be more generators identified as critical assets. However, NERC has not provided any link between imposing additional regulation/costs on a broad swath of additional generation and accomplishing the identified principles. These goals will be best accomplished if NERC issues specific and transparent criteria that identify generation facilities that are truly critical to maintaining BES reliability and then use the industry's expertise to develop cost-effective measures focused to address any identified threat. Thus far the efforts of the SDT have produced useful foundations to help shape a revised set of CIP standards. However, the addition of a sound basis from which to build a structure must also include a cost benefit analysis that is a fundamental tenet of NERC standard development. In addition, it is very difficult to establish the High, Medium, or Low BES impact without the benefit of knowing what the resulting CIP-003 through CIP-009 standards will be. Linking the standard criteria to the reliability and security needs, will enable industry to craft an effective set of cost effective, reliability focused measures. Failing to steer the efforts around a reasonable basis could impose unreasonable costs and produce perverse incentives that may run contrary to reliability goals. Furthermore, the SDT must recognize that it very difficult for an independent generator to fully access whether or not it is critical to the bulk transmission system, and if so at what level. Simply put, generators do not have access to all of the information that is necessary to perform the comprehensive engineering analysis that should be utilized to identify critical assets and correct tier (i.e., High, Medium or Low). Thus it may be more appropriate to assign the obligation to identify critical generation to the Regional Entity (RE) or Reliability Coordinator (RC). Such entities have access to the system data necessary to performing such studies and to making such

Organization	Question 13 Comments (Response page 25)
	determinations. Such determinations should not be made in isolation, but in an open and transparent manner, pursuant to clearly defined NERC standards, and with an opportunity for impacted generators to fully participate in the decision process. II. Comments EPSA's membership supports the use of engineering analysis that is based on scenarios and reasonable assumptions. However, a high-level, bright-line approach is preferable to the SDT. EPSA's membership considered a broad range of potential metrics including geographic location, electric topography, generator performance statistics, and others for the SDT's consideration. Ultimately, while such criteria are useful and could be used to include/exclude some assets in a transparent matter, they are not a substitute for engineering and system operations analysis performed by the applicable reliability authority. EPSA supports the SDT's use of the term Generation Subsystems to define the BES critical assets that can then be categorized through a tiered - High, Medium, Low criteria. However, the concentration and location of generating assets and how that factors into grid topology must also be considered when determining a Generation Subsystem's level of impact. Grid constraints and contingencies play key roles in real-time grid operation, as well as during restoration, making the generation location a significant consideration in determining criticality of Generation Subsystems. In Appendix 1 of the draft standard the SDT provides a framework for how specific subsystems would be categorized. The framework, however, is in some cases subjective or arbitrary (i.e., megawatt level, voltage level, etc) whereas the definitions for High, Medium and Low impact are objective. For example, High BES Impact is defined with respect to preventing system instability, separation or cascade (ISC) whereas the test makes reference to an arbitrary 2,000 MW threshold. EPSA supports the ISC thresholds in the defined terms and suggests the standard be written so that more direct links can be made among the ISC and the tiered approach. EPSA members have discussed at length different threshold measures for determination of the three tiers defined by High, Medium and Low BES impact. Because a bright-line is considered necessary, capacity factor and nameplate capacity were initially considered. These are clearly important factors. However, when system operation and grid topology are considered, size and volume alone do not always provide sufficient linkage to grid reliability or security measures. While a large facility (i.e., greater than 100 MW) with a low capacity factor may not be critical to system reliability, this may also be a factor of the unit's start-up time or ramp rate. A smaller unit with a low capacity factor may be a peaking unit serving an important system reliability purpose. Simply put, nameplate rating and size did not provide a connection to how a generator impacts ISC. Thus, the definitions associated with the tiers and their importance does not provide a sufficient link to the tiered approach in Appendix 1. The location of a Generation Subsystem and how it integrates with the grid can have a much greater impact on ISC and, therefore, needs to play a role in the criteria. For example, a small peaker in New York City might have more significant impact on ISC than a similar facility in a remote area of Montana. Other factors also play a role in determining the relevant tier for a Generation Subsystem. The SDT should provide specific criteria for Black Start units (including units in the cranking path), Reliability Must Run (RMR) units, and possibly any units used to provide non-spin reserves. Since these units can be part of a subsystem, a precise definition for these units and plants will be necessary for identifying and categorizing specific assets. For example, under 1.3 - Pre-designated Reliability Must Run Unit – it is not explained how are units pre-designated. In organized markets will the designation be signified by a contract with the RTO/ISO and a specific utility in other regions? Will such a designation be dependent on the balancing authority? Also regarding 1.4 -Blackstart Generation Subsystem - if there are an excess of Black start units in a BA, are all a part of that Blackstart Generation Subsystem? Providing these distinctions will lead to greater Standard clarity.

Organization	Question 13 Comments (Response page 25)
	Another important factor that should be considered is whether, in the organized market regions, a unit has a capacity obligation (including a unit-specific bilateral contract with a load serving entity). While the presence of a capacity obligation certainly should not be litmus test for categorizing a unit as critical, any unit without a capacity obligation should not qualify as critical, even as "Low" level. Due to the important role the evaluation of a Generating Subsystem's regional location plays in determining its critical impact, EPSA is encouraged by the STD deference to REs playing a role in the determination of generating assets criticality. REs can best utilize other entities such as Reliability Coordinators -- so that appropriate transparent determination can be made. Moreover, the REs are in the best position to evaluate local grid considerations to prevent ISC events. While detailed criteria are appropriate and necessary to ensure consistent determinations of critical assets and tier assignments, an engineering analysis that examines system contingencies, as well as normal and emergency system operation, should be one of the criteria used in making most such determinations. Thus, the obligation to identify critical assets and to identify the appropriate tier must be placed where it belongs – upon the REs and Reliability Coordinators that have the information necessary to conduct a engineering analysis in a transparent manner and to make the determination. Footnote: EPSA is the national trade association representing competitive power suppliers, including generators and marketers. These suppliers, who account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities serving global power markets. EPSA's 21 member companies each operate in four or more NERC regions and represent over 600 registered entities in the NERC registry. The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.
Dynegy	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. As a member of the Ballot Body, I will not even consider voting to approve this Standard unless Version 4 of CIP-002 and Version CIP-003 through CIP-009 are voted upon/balloted at the same time. We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA it is also registered as BA ? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation.
GSOC/OPC	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity

Organization	Question 13 Comments (Response page 25)
	provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards. 2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary? c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could

Organization	Question 13 Comments (Response page 25)
	be lowered if certain protective criteria were met (encryption etc.). 5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas should produce a superior set of standards. 6. With respect to section 4.1 of the Standard, the second sentence, beginning “In situations where . . . ,” should be deleted as unclear and unnecessary.
Hayden	1. I'd suggest that this standard also be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version be addressed completely (including recognition of consequences of new changes). 2. What about "non-routable protocols" and their inclusion/exclusion under CIP-002-4? For instance if you expand the standard to all protocols then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems" and as such this could be a large change to the Registered Entities that it would be difficult for them to become compliant. 3. The Frequently Asked Questions (CIP-002, Question 11) notes that communications systems are not included in CIP-002; however, the new definition of Cyber Systems now includes the "communication" element. Suggest expanding this discussion to address whether or not communications systems are included or not in CIP-002-4. 4. R2 of CIP-002-4 does a good job about having Registered Entities exchange information on BES systems to transmission system owners directly connected to the subsystem. Perhaps this would be a good opportunity to highlight rules/expectations for jointly managed facilities and how "memorandum of understanding" can also be prepared between these Registered Entities that address key requirements such as key responsibilities, definitions of physical and logical boundaries, etc. 5. Does CIP-002-4 change the original Frequently Asked Question response that HVAC, environmental systems are not included in the "Critical Assets" (now BES Cyber Systems)? 6. In question 13 of the FAQ for CIP-002 alarm systems are potentially excluded from the protection as a Critical Cyber Asset. However, with the new definition of a Cyber System, are alarm functions included? (As a note, if an alarm system is "hacked" or fails and results in operators not recognizing negative impacts to the BES, I would argue that these systems should be treated as Critical Cyber Assets.)
SDGE	Attached are suggestions to include for High BES Impact for Transmission Subsystem: - Substation is essential for regulation of Bulk Power voltage - Loss of the substation (all busses greater than 200 kV) may result in voltage less than 90% of nominal, or thermal overloads in excess of 110% of applicable ratings (to be studied at forecasted 50/50 annual peak loads) - Loss of substation may result in voltage collapse or non-localized cascading system outage resulting in more than 100 MW of load loss

Organization	Question 13 Comments (Response page 25)
	- Is the substation essential for black start restoration - Does the loss of the substation result in the loss of critical generation - Is the substation essential for frequency support (can it result in under-frequency load shed or frequency related instability) - Is the substation essential for stability (does the loss of a substation result in loss of resources greater than largest G-1; is the substation essential to an SPS needed to avoid instability, uncontrolled separation, or cascading outages) Attached are suggestions to include for High BES Impact for Generation Subsystem: - Is the generation essential for voltage support and frequency response (is it needed for voltage stability; can the loss of generation result in voltage collapse; can the loss of generation result in underfrequency load shed) - Is the generation essential for black start restoration In Attachment 1, section 1.6 refers to the Transmission Subsystem comprising Black Start Cranking Paths. Does this include 69 kV and 138 kV substations? In Attachment 1, section 1.13 and 2.5 state "… would have an Adverse Reliability Impact." Please define and if this refers to "High BES Impact", state as such. In Attachment 1, section 1.12, we recommend replacing "Cascading outages" with "non-localized cascading outages resulting in over 100 MW loss of load."
APPA	APPA Task Force Prefatory Comments: The APPA CIP Task Force supports the general framework for BES cyber-security proposed by the CS706 Standards Drafting Team ("the SDT") and commends the team for its work. While we have checked "Disagree" for many of comment boxes above, in each case we have attempted to provide constructive comments to improve upon the clarity and quality of the draft standard and where possible, to simplify the steps that registered entities must undertake to ensure both BES cyber-security and auditable compliance. APPA Task Force Comments: Independent 3rd Party Review The APPA Task Force is encouraged by the tiered approach to cyber-security proposed by the SDT, but is concerned that any bright-line metrics must be based on operationally sound regional parameters for BES planning and operations. We agree that use of entity-specific parameters concerning the classification of BES systems should be avoided, because this triggers the same difficult study issues that proved problematic during the identification of Critical Assets under CIP-002-1. However, while the need for entity-specific studies is reduced by using "bright line" regional metrics such as Contingency Reserves and IROLs that define normal and emergency operations, we cannot completely eliminate the need for entity-specific and sub-area studies. Many regional "fill-in-the-blank" standards raise similar issues. For example, the UFLS Standard Drafting Team, in its efforts to determine who should perform region-specific UFLS studies (e.g., to determine how much load to shed at what frequency and with what time delay), has considered a proposal to create a new Registered Entity called the "Regional Planning Coordinator Group." For these reasons, the APPA Task Force recommends that the CSO706 SDT propose to create a new Registered Entity called the

Organization	Question 13 Comments (Response page 25)
	"Regional Planning Coordinator Group." Similar in concept to a Reserve Sharing Group, all of the Planning Coordinators in a region would be required to become members of the Regional Planning Coordinator Group and would be required to perform and/or approve regional studies. The Regional Planning Coordinator Group would also be charged with the review and approval of studies by individual Registered Entities that propose to depart from the regional parameters and bright-line criteria approved under Attachment 1. The SDT should also describe the criteria that the Reliability Assurer will utilize to approve the assessment methods. Please note that the APPA Task Force understood "Reliability Assurer" to be a function performed by the Regional Entity. However, we are unclear how this functional responsibility can be distinguished from the Regional Entity's functional responsibility as the Compliance Enforcement Authority. The approach outlined above addresses regulatory directives that NERC standards not assign responsibility to comply with standards to the same entity that is responsible for assuring compliance with standards, while ensuring that the entity or entities responsible for performing regional studies have a wide-area perspective and the capability to fully assess the impacts of planning and operating studies. The Process for Industry Approval of CIP-002-4 Must be Synchronized with CIP-003-4 through CIP-009-4. We believe the industry the industry will find it difficult to reach consensus in support of CIP-002-4 and address all of the technical issues raised by this standard prior to its review of the associated security controls being developed standards CIP-003-4 through CIP-009-4. CIP-002 through CIP-009 cannot be taken one at a time. The APPA Task Force recommends that the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment. Under this revised development plan, the industry will have the opportunity to understand the whole suite of standards before they vote to give final approval to CIP-002-4. The APPA Task Force would support an industry-wide straw vote to garner conceptual approval of the next version of CIP-002-4 standard. Once so approved, the draft CIP-002-4 could be provided to the FERC and other regulatory bodies either on an informational basis or for conceptual approval. Such conceptual approval by industry and regulators would give the industry, the SDT, regulators and Congress greater confidence that NERC is making strides to complete this project expeditiously, while ensuring that the target end-state will be acceptable to stakeholders and government authorities. Responsibility for Jointly Owned and Operated BES Systems and Cyber Systems: CIP-002-4 should ensure that entities with joint ownership of BES Cyber Systems and associated Facilities coordinate their efforts to comply with the standard. Furthermore, CIP-002-4 should result in the identification of only one responsible entity for each BES Cyber System, and provide that only entities responsible for a BES Cyber System are required to comply with CIP-003-4 through CIP-009-4. Our reasoning is as follows: there are many cases in which multiple registered entities own a BES Facility, while only one of the co-owners owns and operates the associated BES Cyber System.
Consumers	Comment #1: Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in "version 3" to the approach in "version 4" is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be

Organization	Question 13 Comments (Response page 25)
	in scope. Comment #2: We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be interpreted to be in scope in version. Comment #3: We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable. Comment #4: Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. Comment #5: There are multiple alternatives for blackstart cranking paths. The standard needs to specify the “primary” cranking path. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the “primary” cranking path should not be considered as high or medium impact BES Subsystems. Comment #6: Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009 being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. We are not against this narrowing of the standard and believe that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. We have made a number of edits around this position and we hope that the SDT includes them in the next posting. We offer up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical)

Organization	Question 13 Comments (Response page 25)
	1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment 1 if they perform an engineering evaluation / assessment that satisfy Requirement 2. R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…” 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by the responsible entity.

Organization	Question 13 Comments (Response page 25)
	(Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) 2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (We Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entity are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit. 1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL.

Organization	Question 13 Comments (Response page 25)
	1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: We removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? A transmission-only company would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or generation) We believe strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)
NPCC	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline
SWPA	The Applicability Section should be changed to delete Section 5 "Physical Facilities" and replace it with the language currently found in CIP-002-2, Applicability Sections 4.2.1 and 4.2.2 which state that facilities regulated by the NRC are exempt as well as those cyber assets

Organization	Question 13 Comments (Response page 25)
	(or BES cyber systems) associated with communication networks are exempt. The industry should not have to vote on CIP-002-4 prior to the development of the security controls which will apply to facilities or systems included in the scope of CIP-002-4. The standards that delineate the scope of facilities covered and the standards which delineate the security controls to be applied should be voted on as a package. If not, then the effective date of proposed CIP-002-4 should explicitly state that CIP-002-4 should be approved concomitantly with the effective dates of whichever standards are developed which apply security controls to this proposed standard. For the proposed definition of Cyber System: Is it up to each entity to determine whether underlying systems are a part of a given discrete system? Does each "Cyber System" necessarily consist of all its support systems? For the proposed definition of High BES Impact: Who performs the implied risk analyses? Will they be quantitative or a qualitative analyses? Who determines what level of risk is acceptable? How is this risk calculated? Who may accept residual risk? Who may authorize risk transferral? What risk analysis method will be used? In the field of Information Security, the word "risk" has a very specific meaning. If the full power to properly manage its risk is not granted to entities, another word should be used. The standard should contain a “no impact” category. Alternatively, any facilities included in the “low impact” category should not have security controls applied to them as they have no direct adverse impact to reliability. The industry should concentrate on those systems/facilities which potentially have a high impact to reliability. FERC Order 706 told NERC to consider the NIST framework. We strongly support that recommendation; the NIST 800 series allows flexibility in its implementation and acknowledges at its core that "one size fits all" cyber security approaches are doomed to failure. The NERC CIP standards are a compliance-based requirements framework; the NIST 800 series is risk based grounded in performance measurement and residual risk acceptance. The distinction is very important. Even though all traces of the word "risk" may have been scrubbed from the proposed CIP 002-4 draft, the fact will remain that cyber security is inherently all about risk management- it is impossible to remove the concept of risk management from an effective cyber security program. The more the CIPs evolve, the more they are beginning to resemble a reinvention of the NIST wheel. However, the most glaring departure from the NIST approach is demanding that there be zero leeway for entities to assume any risk whatsoever, yet at the same time placing the burden of securing the BES in its entirety upon each individual entity. The proposed CIP 002-4 draft uses a "high/medium/low impact" approach like FIPS-199, which is the document that provides security categorization guidance for the subsequent implementation of the NIST-800 series. The very fact that different levels of "impact" exist means that the unavailability of different systems has differing results on the Bulk Electric System. This is called risk categorization. NERC can rename it to anything they wish, but it is still risk categorization. In keeping with the NIST approach being grounded in performance measurement, the Version 4 CIP standards would be a good candidate for a proof-of-concept demonstration of NERC’s results-based standards (Project 2010-06).
MPPA	Recommend tightening the definitions as well as ensuring that they are consistent with other non-cyber standards. MPPA is very concerned about having to approve standards foe the HML model, without know what compliance is required at each level. MPPA supports approval of the standards as a complete set.
Central Lincoln	Other Comments not already provided in response to earlier questions: We understand the other CIP standards will also be revised. We

Organization	Question 13 Comments (Response page 25)
	are somewhat in the dark in commenting, since we don't know how the categories will ultimately be used in the other standards. We hope that the ballot of CIP-002-4 will be concurrent with version 4 of the other CIP standards so that we will understand the full implications. We understand the SDT is attempting to write a standard that provides brighter line than the prior versions. The proposed revision does not yet hit that mark, but we are hopeful that industry comments will help in this regard. At the same time, we are concerned that the fast track this standard is on will shortcut the comments and the resolution of those comments yielding a standard that has dimmer lines than what is intended.
TransAlta	It is understandable that the draft team adopt high, medium, and low BES impact approach to categorize BES cyber system in order to "allow for requirements that are commensurate with the potential impact". But this can only be supportive in a condition that the cyber security controls to be drafted in the CIP-003 to CIP-009 would be properly assigned to the BES cyber systems based on their level of BES impacts.
NERC	1. It would appear appropriate to tie the effective date of CIP-002-4 to the regulatory approval of the remaining CIP Standards; 2. modify the Physical Facilities section to read "All BES facilities, (including those structures, systems, and components that are Balance of Plant "support systems" that do not adversely impact nuclear safety, security and emergency preparedness within a nuclear generation plant as defined by agreements between the ERO and the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission)." 3. The use of the opt-out engineering and assessment-based methods in Attachment 1 significantly dilute the objective bright-lines being sought, and leave the standard subject to fair criticism for being self-deterministic. Much clearer lines of delineation are needed and one way to accomplish this is to remove the engineering evaluation piece with the associated RC or Reliability Assurer oversight. This by itself would go a long way to keeping the lines clearer. 4. Applicability – if a Reserve Sharing Group has cyber assets that help it function, then it needs to be included in the list. 5. Measure M1 could be more direct: The Responsible Entity shall have a dated and categorized list of BES Subsystems as required by R1. 6. The approach is a significant improvement over the current standard. The standard is definitely heading in the right direction and we welcome the opportunity to support the team in accomplishing its objectives.
Dominion	In preparing these comments, Dominion has made assumptions that will likely be impacted by revisions to the content of standards CIP-003 through CIP-009 that are not yet available. Dominion suggests that once those revisions are available industry participants be provided with another opportunity to review and comment on this CIP-002 proposal. Generally, Dominion has concerns with removing the "routable protocol" language in the existing CIP-002 R3 standard. Entities have based current compliance activities on this language, and removing it significantly expands the scope of the standard to all cyber systems. It is unclear whether removing the "routable protocol" language will result in a corresponding improvement in BES reliability. Attachment 1, item 1.3 says - Each Generation Subsystem that has been pre-designated as Reliability "must run" units. Comment: As it pertains to this standard, Dominion disagrees with classifying Reliability "must run" units as high. In organized markets, such designation usually occurs only when a generator retirement is announced. When this occurs, organized markets have mechanisms

Organization	Question 13 Comments (Response page 25)
	to incent either the development of transmission or generation to allow the retirement of the generator as requested by the owner. This queue process is typically complete within 2-5 years, but it may take longer. Therefore, this designation is short term (2-5 years) in most cases. This short time frame may not allow the owner to implement the changes necessary to comply with the CIP standards before it would subsequently be allowed to retire. If this requirement is kept, Dominion suggests that it be modified so that the entity making the designation has a commensurate obligation to provide the term of such designation. In addition, the requirement should be further modified to allow the owner sufficient time to become compliant with CIP standards.
Encari	No
SCE	SCE believes that NERC should not conduct balloting on CIP-002-4 until the NERC Standards Drafting Team has prepared the revisions to CIP-003 through CIP-009. The categorization of the BES Cyber System cannot be properly conducted in a vacuum that does not consider the Security Controls that will be associated with the categories. We encourage NERC to accept FERC's advice that it is illogical for NERC to rush through CIP-002-4 when NERC has already been informed that NERC and the industry will have to await the completion of CIP-003 through CIP-009 before FERC will rule on the entire set of revised CIP Standards. We appreciate NERC's efforts to CIP-002-4 to date and believe that balloting the standard along with its accompanying suite of CIP standards would be ensure that NERC's efforts are most productive. Combining the voting periods for CIP-002-4 with the other CIP standards would also allow NERC to provide for a clear Implementation Plan for CIP-002-4. It is unclear how an implementation plan can be crafted in the absence of completed revisions to CIP-003 through CIP-009.
USBR	General Comments concerning the Standard: We believe the proposed changes will further complicate identification of critical cyber assets and place additional burden on the industry with little defined results. Furthermore, we are concerned with the proposed passage of a single standard without clear idea of what changes and modifications are going to be proposed for the remaining interconnected standards. We cannot agree to something when we do not know what the defined outcome or requirements are. It feels as if CIP-002-4 is being accomplished in a vacuum without a global understanding of the entire body of requirements. Recommended language adjustments for the SDT to consider: Definition Current Text: Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy. Recommended Change: Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and[inset"/or"] Control Center) used to generate energy, transport energy or ensure[delete "ensure"][insert "directly support"] the ability to generate or transport energy.

Organization	Question 13 Comments (Response page 25)
	Issue/Rationale: The use of the “and/or” language is more consistent with the remainder of the sentence. The use of the term “directly support” does not presuppose that the facility(ies) in question are essential. Definition Current Text: Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: Recommended Change: Control Center — A Control Center [delete "Control Center"][insert "centralized BES operations center that"] is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: Issue/Rationale: Current language uses the same term it is attempting to define. Definition Current Text: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems Recommended Change: • Supervisory control of BES assets, including generation plants, transmission facilities, [insert "and"] substations [insert"/switchyards"] • Automatic Generation [insert "and Voltage"] Control systems or automatic load-shedding systems Issue/Rationale: Separate out individual Control Center functions rather than grouping in this manner. AGC and Load Shedding are not necessarily considered “Supervisory Control” as much as they are automated control systems (alternatively, define “supervisory control” from the perspective of automated controls.) Consider adding voltage or VAR control to the list. Requirement R1.1 Current Text: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. Recommended Change:

Organization	Question 13 Comments (Response page 25)
	The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion [delete " completion"] [insert "effective in-service date"] of the change. Issue/Rationale: The Subsystem could be in-place and in-service for an extended period of time before it is considered “complete” or is even “commissioned.” We suggest the drafting team close the loophole. If the subsystem is complete enough to be in-service, it is complete enough to list. Requirement R1.2 Current Text: The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1. Recommended Change: The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the [insert "required"] categorization of BES Subsystems where required by [delete "where required by "][insert "as outlined in"] Attachment 1. Issue/Rationale: The language is unclear. It is not easily determined if an engineering evaluation is also a part of the work required under Attachment 1 Requirement R2 Current Text: (Not cited) Recommended change: Add language indicating that information exchange with partners should be conducted in accordance with proper Critical Information Protection procedures. Sub-requirement R2.1 Current Text: Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies) Recommended Change: Be more specific regarding “other identifiers.” Specifically, what information is required for each identified BES Subsystem? Requirement R3.1 Current Text:

Organization	Question 13 Comments (Response page 25)
	Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Recommended Change: Define “adversely impact” in terms of the BES. The terms used here and in Attachment 2 place no measures on what constitutes “adverse.” Consider defining “adverse” in real terms specific to the regional operating criteria. Violation Severity Levels For Requirement R2, Severe Current Text: The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization for more than 90 days after the categorization. Recommended Change: The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its [delete "its"][insert "the"] impact [insert "categorization of its BES subsystems"] for more than 90 days after the [delete "categorization"][insert "date these Requirements become effective, or the effective service date of any new BES Subsystems, as appropriate"]. Issue/Rationale: The language is unclear and readily misinterpreted. As written the language could result in NERC having no ability to penalize entities that simply never did a categorization of subsystems under this Standard (and therefore did not notify partners after they completed a categorization.)
Dyonyx	Great job by the Standards Drafting Team! In summarizing our comments, we believe more definition needs to be made to specific terms used in the draft document as delineated in our comments. In our opinion, every effort should be made to simplify the criteria and make it as objective as possible. In addition, where objective criteria can be used, there should not be any alternatives to use “engineering evaluation or other assessment methodology” to circumvent the specified criteria. For example, any Generation Subsystem “whose aggregate output exceeds the largest value of Contingency Reserve or total Reserve Sharing Obligations” should be absolute, i.e., no exceptions. The same applies to black start Generation Subsystems, cranking paths for Transmission Subsystems, etc. In consideration of the black start units and cranking paths, the restoration plans become quite relevant. More attention needs to be given to the issue of redundancies, multiple black start units and synchronization paths as they relate back to the categorization of BES Subsystems. Lastly, we are very concerned about the industry blessing these changes without having first understood the proposed requirements for the remainder of the standard. For example, how will the Cyber Security Controls be applied to Medium and Low Impact BES Cyber Systems? How will IP-based protocols be considered in the need to apply relevant Cyber Security Controls? While we understand the costs for implementing the standard in the eyes of FERC may not be a consideration, the industry needs to have

Organization	Question 13 Comments (Response page 25)
	a voice in establishing reasonableness such that the provisions of the standard can be met without bankrupting the underlying functional entities. After all, the functional entities have a responsibility for being "prudent" in protecting the rate payers while balancing the application of appropriate security provisions accordingly.
MISO	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. We are also concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The

Organization	Question 13 Comments (Response page 25)
	Commission used the term “external review” in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA if it is also registered as the BA? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation. We are concerned about the addition of the function entity Reliability Assurer. While it was added to the most recent Functional Model, we believe it is premature to begin using this entity. While many believe that NERC and the Regional Entities are ultimately the Reliability Assurer, the function model is not clear this is the case. Furthermore, the Functional Model Working Group purposely drafting the Functional Model in a way so that it does not have to be the Regional Entities and/or NERC. Does the drafting team have a vision of whom the Reliability Assurer is? It has not been shared and we believe the drafting team needs to make clear whom they believe serves this role before it is added as new functional entity. Has this addition been coordinated with NERC certification and registry staff whom will have to register and certify this entity?
Westar	CIP-003 to 009 version 4 should be developed in parallel with CIP-002. They should be developed and voted on as a package.
Green Country	It is a widespread feeling that this standard no matter what its final draft ends up being should only go to vote as a package with CIP-002 thru CIP-009 since they are totally dependant on each other. Get this draft done, present 3-9 drafts for "informal" comment. Develop a final draft package and move on with them as a group.
Oregon PUC	The Safety Reliability Security Division of the Oregon Public Utility Commission appreciates the hard work of the SDT in the drafting of CIP-002-4. We also appreciate the many organizations that support the SDT team members and those that actively comment on this critical standard proposal. We strongly support NERC standards and requirements that bring sound value to the reliability of the electric grid. Standard CIP-002 is a cornerstone standard for which so many other NERC standards and requirements depend. This standard, even more critical than others, needs to be clear, specific and technically defensible. If we don’t get this standard right – utilities, operators, and their ratepayers will suffer the cost of exposure to unending interpretations, corresponding enforcement actions, unnecessary diversion of resources and time away from more meaningful transmission investments. We apologize that we cannot give more meaningful comments at this time. We understand the impacts of CIP-002-4 are far-reaching to numerous other NERC standards, especially CIP-003 through 009. Our concern is that changes to CIP-003 through CIP-009 will have profound financial impacts to utilities and their ratepayers. Until the industry can understand these impacts in whole, we are skeptical of the benefits and costs. We would definitely recommend that the SDT do a benefit-cost analysis for the Low BES Impact Level taking into account probable changes to CIP-003 through CIP-009 standards. Likewise, the SDT should do a benefit-cost analysis for the Medium Level. Also, we recommend that a comprehensive implementation plan be developed for CIP-002-4 Medium and Low BES Impact levels. These levels should have delayed implementation schedules to allow time for compliance in concert with the changes in CIP 003 through 009. The risks associated with the lower levels are lesser so the urgency for prompt compliance is not as great as the high level. We also recommend that CIP-002-4 for the two lower levels be used as a trial-use guide until the next versions of CIP-003 through CIP-009 are approved by FERC. During the trial period, audits should be performed to determine how the CIP-002-4 is interpreted and enforced, but without sanctions.

Organization	Question 13 Comments (Response page 25)
Manitoba 1	no
Portland GE	Portland General Electric ("PGE") has been involved in NERC's Cyber Security efforts since Urgent Action 1200. PGE has identified critical assets for its Balancing Authority, Generation Owner/Operator, and Transmission Owner functions. While PGE appreciates the Standards Drafting Team ("SDT") considering changes to CIP-002 to address FERC Order No. 706 cyber security directed modifications and encouraging industry discussion, PGE has significant reservations about implementing these wholesale changes at this time. Registered entities have devoted significant resources to implement CIP compliance programs to meet the current requirements, and it is simply too soon to scrap those efforts and require entities to start over building new compliance programs to meet new CIP standards. While PGE would support certain improvements to the existing cyber security standards, PGE does not support the complete paradigm shift proposed by the SDT. The SDT has given very little reasoning for the scope of the proposed changes, and cannot justify requiring Registered Entities to start over on CIP compliance at a time when those entities are still building compliance programs to meet the current CIP requirements. To justify the entirely new approach to cyber security regulation proposed by the SDT, the SDT would have to build a record demonstrating the ineffectiveness of the current standards, and no such record exists at this time. To the extent the SDT believes the current standards to be insufficient to protect the reliability of the bulk electric system, the SDT should propose incremental improvements to the existing standards rather than prematurely changing course entirely. For example, if the SDT perceives that registered entities are under-reporting critical assets and/or critical cyber assets, the SDT should determine whether such under-reporting is the result of (1) a lack of clarity in the current requirements, or (2) an effort by Registered Entities to evade their CIP compliance obligations. If the SDT determines that the problem is a lack of clarity in the current CIP requirements, the SDT can clarify those requirements in a manner that should drive entities to designate additional critical assets and critical cyber assets. If the SDT determines that the under-reporting is an effort by registered entities to evade their compliance obligations, that problem would be best addressed through the compliance and enforcement process. Similarly, if the SDT desires to implement a risk management framework akin to the NIST Framework, that too could be accomplished through incremental modifications to the existing cyber security standards rather than by starting over with the approach proposed by the SDT. Prior to imposing requirements on systems and facilities that are not truly "critical" to the reliability of the bulk electric system, the SDT should seek information on how utilities currently protect those systems and facilities. For example, PGE, like most other companies, must follow good utility practice and have cyber-security policies in place to protect all of its cyber assets from just the threats that are contemplated in these standards. The SDT should gather information from entities and build a record supporting the need for moving toward something like the NIST Framework if the SDT believes that such a modification would enhance the reliability of the bulk electric system. While PGE does not support the scope of revisions proposed by the SDT, PGE also finds it difficult to comment on the specifics of the proposed standard without knowing this standard's effect on the current CIP-003 though CIP-009 standards. PGE and other ballot holders are unable to fully evaluate the framework established in CIP-002 without understanding the scope of controls that will be included in the standards that will succeed the current CIP-003 through CIP-009. With the current CIP-002 draft, PGE is unable to determine to what extent the Standards Drafting Team has drawn the lines between "High," "Medium," and "Low" BES Impact, and therefore the full

Organization	Question 13 Comments (Response page 25)
	regulatory impact of these categories is unknown. Additionally, this paradigm shift turns a clearly defined standard, which gives utilities the ability to build risk-based methodologies that work for their particular systems into a standard that is entirely subjective, with few defined terms. This causes great concern, most significantly for auditing and enforcement purposes. For example, “unacceptable risk” is an undefined term, and therefore subjective to each company – and to each auditor. Moreover, it appears that the CIP standards are being developed and revised in a “vacuum,” rather than in conjunction with the bulk of the mandatory reliability standards (“Order 693 Standards”). This could create a “security versus reliability” issue for companies. Clearly, both security and reliability are important and the purpose behind the efforts of the regulators and utilities in implementing the mandatory NERC reliability standards regime. PGE believes there is some risk that the proposed standards could provide a disincentive to utilities to upgrade equipment to enhance communications and reliability because such upgrades could bring the equipment into scope for a higher level of CIP controls. Because they require an independent assessment of a utility’s equipment from those studies already performed under the Order 693 Standards, these proposed CIP standards could set a different – and possibly higher – standard for reliability than the Order 693 Standards. For example, the Transmission Planning Standards (“TPL Standards”) from Order 693 set specific circumstances and planning studies for transmission planning to maintain the reliability of the system. The CIP-002-4 standard as proposed creates an entirely separate regime under which the facilities are assessed. The utilities are then faced with the task of doing separate studies for the same facilities to achieve the same purpose – the reliability of the bulk electric system. The SDT should look to achieve efficiency and consistency between the two sets of standards where possible, and it appears that the proposed standard would, if anything, result in inconsistencies and inefficiencies. Finally, this standard as proposed would create great burden to utilities. Just as companies are finalizing their current CIP compliance programs and, in PGE’s case, preparing for its first spot check of its CIP compliance efforts, they are being asked to weigh in on a completely new approach to CIP compliance. For example, all documentation identifying critical assets or critical cyber assets would require material changes, and the proposed standard would exponentially increase the number of assets considered to have an impact on the bulk electric system, many of which have no communications abilities or any actual potential impact on the reliability of the system. The tracking and reporting requirements included in this standard are not only burdensome, but would also create a substantially higher compliance risk to utilities without necessarily enhancing reliability. PGE recommends that NERC wait until the results of the initial round of spot checks are analyzed before taking such a drastic step to overturn the current regulatory framework. PGE also encourages the SDT to consider the potential compliance risk inherent in such a fundamental change to existing cyber security controls. Companies, including PGE, have invested a great deal of money and the efforts of a large number of employees into establishing compliance with the current standards. Companies including PGE have invested a great deal of money and the efforts of a large number of employees into coming into compliance with the standards as they are written. PGE has spent thousands of hours identifying its critical assets and associated critical cyber assets and developing compliance programs, procedures, and documentation to demonstrate compliance with the current CIP standards. Under the proposed standards, all of the work identifying critical assets and critical cyber assets would be effectively scrapped, and all of the compliance programs, procedures, and documentation would, at a minimum, require substantial changes. The SDT should consider the very real possibility that some individuals and entities will discount the importance of their future CIP compliance efforts if their efforts to date are written off at this early stage in favor of a new regulatory paradigm.

Organization	Question 13 Comments (Response page 25)
	A wholesale paradigm shift to these regulations, especially one that is not clearly written and objectively defined, will lead to confusion on the part of the front-line employees responsible for complying with these regulations. Constant changes to the controls under which people perform their day-to-day tasks could potentially create general uncertainty about which controls are in place and what an employee's obligations are at a given time. The risks of such constant changes to the cyber security regulatory scheme should be taken into account when contemplating a change of this magnitude. Instead of changing courses entirely, the SDT should value the thousands of hours and millions of dollars of CIP compliance work that has been done under the current standards, and work to improve the reliability of the Bulk Electric System through improvements to the existing CIP standards.
PSEG	Comment #1: Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in "version 3" to the approach in "version 4" is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be in scope. Comment #2: We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be interpreted to be in scope in version. This stepping block could be structured as per comment #3, following. Comment #3: We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable Comment #4: Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. Comment #5: There are multiple alternatives for blackstart cranking paths. The standard needs to specify the "primary" cranking path for initial system restoration. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the "primary" cranking path should not be considered as high or medium impact BES Subsystems. Comment #6: Those companies that have made a significant investment in designing Blackstart plans, including multiple cranking paths and blackstart units affording great flexibility and redundancy, should not be effectively punished for having a diverse set of assets available for system restoration. Only primary units and cranking paths used for initial system restoration should be considered as high or medium impact BES subsystems. Comment #7: Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009

Organization	Question 13 Comments (Response page 25)
	being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. We are not against this narrowing of the standard and believe that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. We have made a number of edits around this position and we hope that the SDT includes them in the next posting. We offer up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical) 1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment 1 if they perform an engineering evaluation / assessment that satisfy Requirement 2. R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to

Organization	Question 13 Comments (Response page 25)
	take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…" 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by the responsible entity. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) 2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Comments on Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (We Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached.

Organization	Question 13 Comments (Response page 25)
	In addition, entities are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability “must run” unit. 1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: We removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? A transmission-only company would not know how to apply the 2,000 MW level. (Does this apply to the MW’s of load or generation) We believe strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria:

Organization	Question 13 Comments (Response page 25)
	1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)
WE-Energies	Wisconsin Electric Power Company contributed to and supports EEI's comments regarding this question. Wisconsin Electric Power Company also agrees with comments as put forth by Midwest ISO. In addition Wisconsin Electric Power Company has the following comments: • Two year implementation is too short. A compliance infrastructure did not exist for the generation entities as it did for BA entities, and should allow additional time for compliance activities. • Need to better define the term "under its ownership". Does this include telecommunications systems (telephones)? • The definition of Cyber System does not include the category of control. We further recommend more clarity in the list of attributes. For example, what does "maintenance" apply to? It should not include test equipment and data. • Under High BES Impact, use the NERC Glossary term "Cascading". Also, the term "planning time frame" is not clearly defined. Does this mean we have to make a new assessment for every unit outage and line outage? Recommend removing the language around the planning time frame. • Physical Facilities uses the expression BES facilities and then further expounds by listing "those structures components, equipment and systems of facilities within a nuclear generation plant ...). We're not sure if the intent is to use the NERC Glossary term Facilities which is already defined, or if this is intended to be "facilities." • CIP-002-4 effective date should coordinate with the CIP-003 through CIP-009 V4 effective date. • It is difficult to agree with the direction taken by this standard without examining the impact of how the compliance standards CIP 003- CIP 009 would apply to these asset categories. Wisconsin Electric Power Company recommends a more evolutionary approach which would keep the current CIP-002-2 critical asset and associated critical cyber asset determination and methodology, but enhance it by using the proposed attachment 1 high and medium impact criteria for critical asset determination. • The category Low BES Impact should be dropped - too inclusive. Per the definition, low impact assets have little or no effect on BES reliability. • It is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means.

Organization	Question 13 Comments (Response page 25)
Idaho Power	This draft is a drastic change from previous versions and will require sizable effort from the Registered Entities to comply with proposed changes. A realistic implementation schedule along with comprehensive guidance/assistance is essential to Registered Entities to successfully implement the proposed changes. It would also be helpful to get some idea about what CIP-003-009-4 will look like before gaining approval of CIP-002-4. Compliance with the CIP standards is costly and expanding the scope of CIP in this proposal will make it even more so. Although cost is not an excuse for non-compliance, it is a factor for most entities that requires that we plan and budget for well in advance of a compliant date. We support the position that the categorization of the cyber systems by their impact on critical BES functions is a more straight forward approach and relieves the entities of the burden to categorize all of their BES subsystems. A fairly comprehensive list of the cyber systems that should be considered in the categorization process would be very helpful.
SOCO	Explicit provision should be made for joint ownership of a BES subsystem. The 8 quarter implementation deadline from the date CIP-002-4 is approved is concerning because version 4 of CIP-003 thru 009 will most likely not be finalized and approved until six months after CIP-002-4 is approved. We cannot make implementation plans or actually implement cyber and physical controls at newly identified cyber assets that result from CIP-002-4 without knowing what the required controls will be for the high, medium, and low impact categories. CIP-002-4 is going to significantly increase the in-scope cyber assets associated with Transmission Subsystem assets. We recommend that the 8 quarter implementation deadline start from the point version 4 is approved for all of the CIP standards (CIP-002 thru 009). This comment has already been made and the Substation representatives would like to restate it here. Unless there are no requirements at all for cyber systems associated with Low BES Impact Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all Low BES Impact Subsystems should be exempt from the CIP-003 through CIP-009 standards or a category for minimal-risk or no-risk subsystems must be created. Voting on CIP-002 apart from being able to see the actual controls required per category is asking the industry to put themselves in the difficult position of determining if the scope and classification is correct before we know anything about what each classification means in terms of security requirements. Breaking the set of standards up and sending CIP-002 to FERC ahead of the other requirements has been unfairly imposed on the drafting team. Lack of 'Bright Lines'. The industry wants ‘bright lines’ in the standard so that compliance state is objectively deterministic and not subject to interpretation in audits. There are two areas where bright lines are still not evident: 1. Defining BES Subsystems. Even though Attachment 1 is striving to provide bright lines for classifying BES Subsystems, there are few to no rules for determining what a BES Subsystem is. An entity and the regulator could define them totally different for any given asset such as a plant. The drafting team itself has gone through exercises with simple plant diagrams and has had numerous conflicting answers on the resulting BES Subsystems in that plant. 2. Defining BES Cyber Systems. The current R3 has almost no lines at all and it’s the crucial one for a cyber standard. It simply asks for a list of cyber systems that can affect any of 9 Reliability functions (with 63 subfunctions listed) in Attachment 2. Pick “Situational Awareness”; what is the bright line that tells an entity or an auditor whether something is or is not part of situational awareness and should be on the list and how does either prove that you have them all? You could make the case that any and every cyber system is part of situational awareness. Next pick the “Control and Operation” function and consider how to provide evidence that you have

Organization	Question 13 Comments (Response page 25)
	every cyber system with any involvement in that on the list. Classification updates. The classification of all BES Subsystems and all BES Cyber Systems is a monumental task. The drafting team is attempting not to have that be a regularly occurring (annual) process but rather do it once and then maintain it as the BES assets and the cyber systems change. However, documenting 'changes in the electric system' and all subsequent classifications for compliance tracking purposes is problematic.
DTE	We think that a tiered approach is a more appropriate way to identify assets than the current Standards, and is also being utilized in other Homeland Security applications/regulations. (CFATS - Chemical Facility Terrorism Standards, MTSA with TWIC readers - Maritime Transportation Security Act & Transportation Worker Identification Credentials proposed rule, etc.) However, we prefer the criteria for asset identification at the various impact levels be established at the same time as the security controls/measures (cyber & physical) that are to be utilized at each level. It is not clear how this will affect CA/CCAs that have already been identified. We are concerned that entities have wasted time, money and manpower. There needs to be guidance on how to leverage work that has been done to protect CCAs in compliance with the current version of CIP. We recommend considering other physical security regulations for facilities that already have existing Facility Security Plans under (CFATS, MTSA, etc.) to eliminate duplication for entities having to comply with multiple regulations. We are concerned on how this change to the standard will affect an organization that may be audited partially under the old standards and partially under the new standards. Editorial Comment: Section A5 Physical Facilities should be under section 4 Applicability so Physical Facilities should be 4.2 and paragraph 5.1 should be numbered 4.2.1. Effective date then becomes number 5.
AEP	No additional comments at this time.
NS&T	We commend the SDT for the time and effort invested in developing the draft standard, and we thank the members for this opportunity to share what we hope are useful comments.
Flathead	I appreciate the efforts of the drafting team to respond to forces beyond their control. In general, this approach comes too close to regulating local distribution assets often not included in registration criteria, drawing staff and resources away from protecting what is truly critical. Encourage the team to limit this rewrite things that meet the medium and high categories.
E ON	Other Comments not already provided in response to earlier questions: E ON U.S. is concerned that CIP-002-4 draft is being proposed “in a vacuum,” without context of the requirements from the other CIP standards. It is one thing to categorize assets as high, medium, or low potential impact, but the real cost in compliance is in the protective measures that need to be implemented in response to this identification and rating of these assets. The cart may have been placed ahead of the horse. More information concerning how high, medium and low impact assets are to be protected is required before industry can reasonably be expected to sign off on CIP-002 V4.

Organization	Question 13 Comments (Response page 25)
	The methodology also seems to address cyber risks in a silo, without an overall risk-assessment of other threats against critical assets that should be considered for proper prioritization and investment in protective measures. It seems that some consideration should be given regarding cost/benefit analysis in meeting a control objective versus the value of the asset that is the target of protection. Future installation of programmable devices intended to enhance BES reliability will be weighed against the cost of complying with the Version 4 CIP standard requirements applicable to such devices. Entities may in fact disconnect existing systems. This may well result in decreased BES reliability. The drafting team appears to presume that the BES as whole, i.e., the BPS grid, the target of protection whenever CIP requirements are mandated for any size facility or associated cyber asset. This can only be true if industry is abandoning not only N-1 analysis but also any realistic attempt at examining reasonable contingencies. The standard appears to assume all of an entity's assets can be simultaneously compromised. The costs that are certain to result from this assumption demand that the assumption be challenged and debated not only by registered entities but by regulators at all levels responsible for protecting utility ratepayers.
Carthage	Please clarify All BES Facilities in section 5.1 of the standard. Is this intended to mean the facilities operated at 100 kV and above as the BES definition states? CWEP feels that there should be a category for No BES Impact as stated in number 8 above. CWEP feels that the CIP-002 thru CIP-009 Version 4 standards should be approved as a package so entities have a chance to review the requirements of CIP-003 thru CIP-009 before CIP-002 is implemented. The effective date of CIP-002 thru CIP-009 should be the same. CWEP feels that there should not be any mandatory controls for facilities that are low impact and have no communications. Again CWEP is okay with the format of the standard but would like for the criteria to be more specific. CWEP feels that applicability needs to be clarified throughout the standard to ensure that it's interpreted correctly as stated in numbers 8 and 12 above. CWEP feels that this could help eliminate any unnecessary confusion. The standard is very confusing as to whether it is intended to apply to smaller entities. Smaller entities being systems that operate at less than 100 kV. CWEP feels that the standard, as written, has the potential to place a considerable burden on smaller entities and not achieve much in the way of reliability. CWEP would like to request that clearer lines be established so that entities understand if the criteria applies to them or not.
WECC	We feel that attempts to limit analysis to only an impact based analysis has left things dependent on engineering study's and makes it actually more difficult to determine criticality. We feel that moving to a high, low, and medium impact is best done by bringing probability of an event back into the criteria. We do not agree with NERCs intent to remove probability from the risk assessment process, particularly with the return to classifying assets as high, medium and low risk.
Entergy	Comments and Recommendations Concerning Draft CIP-002-4 • Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective.

Organization	Question 13 Comments (Response page 25)
	• The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. • Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. • CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. • The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… • The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below. Validity of the "Cyber First" Approach to Defining Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – system stability is the salient issue. • N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a coordinated multi-site attack, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on a perpetrator's ability to navigate across and between control system data networks in order to access multiple sites. • "Routable protocol" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented). • Thus, routable protocol networks are the correct object of cyber protection concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.] • At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means. • CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for all control system cyber assets that communicate in common on a TCP/IP-based data network infrastructure; regardless of how big or small the grid operating site is in terms of electrical rating. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities

Organization	Question 13 Comments (Response page 25)
	relevant in practice to BES reliability. • If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is not for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not be imposed where cyber threat is not real. • Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the different Categories of cyber assets as characterized below. Identifying Specific Cyber Objects of Protection • Start by identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement, execute, or support the Essential Functions. • Generally speaking, process and distributed control system elements at work at different types of grid operating site present three major cyber asset categories in terms of cyber risk exposure to the bulk electric system: o o Category 1 (High): Control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate; these require the most rigorous cyber security controls and countermeasures because nefarious root capture of control system hosts represents the worst case scenario. o o Category 2 (Medium): "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use. Dial-up aside herein, these cyber assets require earnest cyber security controls and countermeasures, but nefarious root capture of same typically does not directly represent the same grid threat severity as do control system host computers themselves. o o Category 3 (Low): Cyber assets in use at all other operating sites that do not employ routable TCP/IP protocols to communicate. These should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc). • Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset identified above. More granular refinement of cyber security control and countermeasure Requirements will be necessary beyond the gross categorical illustration above, especially concerning Category 2. • Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not in terms of facility size/rating] • All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I. Advantages of the Recommended Approach • It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The

Organization	Question 13 Comments (Response page 25)
	subject is computers, not electricity. • This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's complimentary improvement, not do-over. • It results in application of cyber defenses appropriate to true risk, and does not require expense and effort securing assets that do not pose a genuine vulnerability/threat. • It provides Responsible Entities the autonomy to manage gradual replacement of antiquated data networking in favor of high performance TCP/IP networking that demands more rigorous cyber security controls and countermeasures. • It buys the industry time to appreciate the impact of Smart Grid and NASPI on security controls/countermeasures needs prior to upgrading control systems networking.
CenterPoint	The proposed security control measures for CIP-003 – CIP-009 and overall implementation plan for Version 4 should be provided prior to voting on CIP-002.
LCRA	Question - 8. D. Compliance, 1.3, bullet 1 – Does the phrase "last update" include the annual review? If the document is reviewed each year but not changed, is there a requirement to keep all old copies or just the most recently reviewed copy?
FRCC	In Section D, Compliance, Item 1.1.1 is not clear to me. I believe the drafting team is trying to say that if a Regional Entity is registered for a specific function, such as RC etc, then the Regional Entity can not monitor themselves. If not, I am confused with the use of the term Responsible Entities. For instance, the FRCC is registered as a Reliability Coordinator. The FRCC Compliance Staff does NOT monitor the FRCC RC as identified in the delegation agreement. But, the FRCC RC function does utilize an entity as an agent to perform the RC function. The FRCC Compliance Staff does, and should be able to monitor that particular entity for their own registered functions that are separate and apart from the function that they perform as the agent for the FRCC RC. And, 1.1.2 states that the ERO is the monitor for a Regional Entity. That does not have to be the case. FERC through the delegation agreements has allowed for other 3rd parties to be the monitor for a RE. I would suggest that this Compliance Enforcement Authority section just be revised to state that it would be per the ERO Rules of Procedure and the NERC/Regional Entity Delegation Agreements. The Reliability Standard should not dictate something that may be in opposition to what FERC or other governmental authority has allowed.
NIPSCO	Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in "version 3" to the approach in "version 4" is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be in scope. We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be interpreted to be in scope in version 4. We suggest that a new intermediate version 4 simply take the existing version 3 and modify CIP-002-3 R1.2 to include some of the specific items in the draft CIP-002-4 attachment 1 document. This approach would result in a new version 4 with an expanded Critical Asset scope, a new implementation plan, and would act as a step between V3 and the proposed V4.

Organization	Question 13 Comments (Response page 25)
	We also believe that this stepping block approach should address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that this new version 4 should include language addressing the final approved interpretations (RFI's) from previous versions.
ConEd	The associated Guideline on page 10 of the document states: "In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems." The Guideline provides an example for the SCADA system that causes the Control Center High rating to overshadow the other subsystems. It is not clear whether or not the SCADA (which would be a HIGH) would become so due to its control of all BES substations and generation plants through the station RTU devices cause all these "associated" subsystems to become HIGH by inheritance, or not. The intent of this requirement may have significant impact to our classification criteria if the SCADA causes other system to become rated HIGH • Attachment 1, item 1.5: what does "transmission lines leaving the station" mean? Suggest saying "transmission lines connected to the station". • Attachment 1, item 1.1: 'exclusion' does not make sense - if a generating plant is determined to "not be essential to the reliability of the BES", then why does it default to Medium? If the plant is not essential, it should either be categorized Low or excluded. Same comment applies to 1.5. • Attachment 1, item 1.2: Change "output" to MVA nameplate rating. Add "in the relevant RC region" to the end of the sentence. • Attachment 1, item 1.5: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 1.5: last sentence is missing the ending that appears in 1.1: "...in which case such Subsystems may be categorized as Medium BES Impact." • Attachment 1, item 1.10 and 1.11: this language seems to imply that each and every combination of substation needs to be evaluated to determine if the loss of that aggregate subsystem would have on frequency and voltage. Is this the drafting team's intent? • If Transmission Subsystem consists of one or more elements, how does an entity demonstrate to an auditor that all combinations of transmission subsystems were evaluated? For example if an entity owns 20 345 kV substations, do you have to evaluate every combination of the 20 as a separate subsystem? • Attachment 1, item 2.2: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 2.2: replace "they" in 4th line with "the Transmission Subsystem"

Organization	Question 13 Comments (Response page 25)
	• Attachment 2, Dynamic Response: spell out the word “Transformer”. Do not use abbreviation x-former. • Attachment 2, Managing Constraints is missing the word "function" in the second paragraph. R3.1: Each Responsible Entity shall list each BES Cyber System (associated with a BES Subsystem categorized in Requirement R1) that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Need to clarify that the "that" in R3.1 refers to BES Cyber System and not to BES Subsystem, perhaps by including the parenthesis added above. The Drafting Team has developed a “bright line” approach for categorizing BES Subsystems. In lieu of this approach, the Drafting Team is encouraged to consider use of an impact-based methodology, reviewed and approved by the Reliability Assurer, such as the NPCC A-10 Criteria. The Drafting Team should consider an “NA” (“Not Applicable”) designation for elements that fit the BES definition, but have NO impact on Interconnected Bulk Electric System. This designation would be "below" an even LOW impact level, allowing Entities to reflect the accurate impact/status of some of its system.
EEI	1. EEI supports NERC’s efforts to develop a complete revised set of CIP standards in 2010, with a plan to file the new set of Standards with FERC in early 2011. EEI and its members recognized the importance of this activity and are committed to this effort. EEI believes that the new CIP standards development project is one of the most important activities facing both NERC and the industry in 2010. 2. EEI believes that NERC can put forward a single package that includes both the proposed standard for BES Cyber System Categorization, as well as the associated controls. This will allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of associated controls. 3. EEI agrees that there is value in identifying clear and straight forward bright line criteria for high, medium, and low impact BES assets. The bright line criteria should be subject to an approved engineering evaluation in the event that an entity owns or operates an asset that while meeting certain criteria, does not affect the BES to the level indicated by the bright line. 4. EEI believes that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility exceptions (TFEs). 5. EEI believes that the current written definitions for high, and medium impact BES systems do not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in Appendix 1 to make such determinations. 6. EEI suggests that the drafting team use terms and definitions that exist within the NERC Glossary whenever possible, and avoid the use of vague language that may lead to subjective interpretation. 7. EEI believes that this SDT needs to be very clear that this standard can only apply to those facilities that are covered under FPA 215 as defined by the definition of BES. 8. Moving into the future, a. EEI believes that standards development team should focus on the “What” of security control outcomes rather than the

Organization	Question 13 Comments (Response page 25)
	"How". b. EEI suggests that the drafting team carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
O&R	The associated Guideline on page 10 of the document states: "In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems." The Guideline provides an example for the SCADA system that causes the Control Center High rating to overshadow the other subsystems. It is not clear whether or not the XA21 SCADA (which would be a HIGH) would become so due to its control of all BES substations and generation plants through the station RTU devices cause all these "associated" subsystems to become HIGH by inheritance, or not. The intent of this requirement may have significant impact to our classification criteria if the SCADA causes other system to become rated HIGH • Attachment 1, item 1.5: what does "transmission lines leaving the station" mean? Suggest saying "transmission lines connected to the station". • Attachment 1, item 1.1: 'exclusion' does not make sense - if a generating plant is determined to "not be essential to the reliability of the BES", then why does it default to Medium? If the plant is not essential, it should either be categorized Low or excluded. Same comment applies to 1.5. • Attachment 1, item 1.2: Change "output" to MVA nameplate rating. Add "in the relevant RC region" to the end of the sentence. • Attachment 1, item 1.5: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 1.5: last sentence is missing the ending that appears in 1.1: "...in which case such Subsystems may be categorized as Medium BES Impact." • Attachment 1, item 1.10 and 1.11: this language seems to imply that each and every combination of substation needs to be evaluated to determine if the loss of that aggregate subsystem would have on frequency and voltage. Is this the drafting team's intent? • If Transmission Subsystem consists of one or more elements, how does an entity demonstrate to an auditor that all combinations of transmission subsystems were evaluated? For example if an entity owns 20 345 kV substations, do you have to evaluate every combination of the 20 as a separate subsystem? • Attachment 1, item 2.2: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 2.2: replace "they" in 4th line with "the Transmission Subsystem"

Organization	Question 13 Comments (Response page 25)
	• Attachment 2, Dynamic Response: spell out the word “Transformer”. Do not use abbreviation x-former. • Attachment 2, Managing Constraints is missing the word "function" in the second paragraph. R3.1: Each Responsible Entity shall list each BES Cyber System (associated with a BES Subsystem categorized in Requirement R1) that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Need to clarify that the "that" in R3.1 refers to BES Cyber System and not to BES Subsystem, perhaps by including the parenthesis added above. The Drafting Team has developed a “bright line” approach for categorizing BES Subsystems. In lieu of this approach, the Drafting Team is encouraged to consider use of an impact-based methodology, reviewed and approved by the Reliability Assurer, such as the NPCC A-10 Criteria.
Alliant	It is imperative that the rest of the CIP standards be developed before CIP-002 is balloted. We can not make an informed affirmative vote on this standard until we know what the controls will be for "High", "Medium", and "Low" impacts. There must be a "Not Applicable" selection of Impact as well. There are some cyber assets that have no impact on the BES, and that must be recognized. We believe there should be more clarity for what constitutes a cyber attack. The Standard needs to further clarify if it is protecting against singular or wide-spread attacks, or both.
Ameren	This current draft does not address the FERC concern of the industry being prepared to respond to "coordinated attacks”. It just appears to provide for a more consistent application of the current standard only. There needs to be a matrix approach to develop a list of high impact BES Subsystems that have high impact BES Cyber Systems required to be protected. How would protecting a low impact BES Cyber System in a high impact BES Subsystem improve the reliability of the BES, for example protecting a BES Cyber System that does not use TCP/IP or dialup accessible? There is no wording in this draft addressing the subject of “misuse” as dictated in FERC Order 706. It is hard to evaluate this standard without seeing the remaining CIP standards, CIP-003 through CIP-009 for security controls. Terms used in this draft of CIP-002 that are not defined in the NERC Glossary of Terms need to be added. For example; “Regional Reliability Assurer”, “adversely impact”, “unacceptable risk”, “instability”, and “shared element” Remove the definitions of High, Medium, and Low BES Impact in this standard and use only Attachment 1 for these definitions. Clarify how to utilize attachment 2 or add more criteria for defining BES Cyber System that have the potential to adversely impact any of the functions identified in CIP-002 Attachment 2. For example what about BES Cyber Systems that are not dialup accessible or do not use a routable protocol. How do these systems have the potential to adversely impact any of the functions in Attachment 2 if they are not remotely accessible? There needs to be definition of what is an acceptable engineering assessment that can be used to determine the BES impact categorization.

Organization	Question 13 Comments (Response page 25)
Black Hills	Concern that rigorous implementation of CIP-002-4 as currently described would dramatically increase the amount of BES sensitive information that would be shared among entities and consultants, which increases the possibility of that information being compromised or abused.
TNMP	TNMP has concern regarding retirement of the definition of "Cyber Assets." TNMP cannot envision how future versions of CIP-003 through CIP-009 will be applied with just the BES Cyber System definition. If the drafting team is preparing a paradigm shift permitting devices within an ESP but not part of a Cyber System to be exempted from CIP requirements, then the definition is not necessary. However, if the goal is to continue CIP protection of all Cyber Assets within an ESP containing a BES Cyber System, then the definition must be kept. If the term Cyber Asset is to be kept then TNMP would like a revision to the definition removing the phrase "and data."
NVEnergy	We commend the drafting team on their work thus far. This draft represents sweeping changes and paradigm shifts in the way critical infrastructure protection is to be handled. The draft revisions are heading in the right direction; i.e., applying a varying degree of security objectives upon those systems that have the highest degree of impact; however, the standard should focus on those accessible (routable protocol, IP, dial-up) cyber systems that have impact upon the reliable operation of the BES. Critical Assets, Critical Cyber Assets and Cyber Assets are terms that would be retired from the Reliability Standards Glossary of Terms. As such, upon implementation of CIP-002-4, all other CIP Standards (CIP-003 - CIP-009) would become defunct and/or unenforceable. The CIP-003 - CIP-009 Standards rely on the definition of Critical Assets, Critical Cyber Assets and Cyber Assets to define what needs to be protected, the level of protection required, the required security management controls, training and review, establishment of electronic security perimeters, physical and system security requirements, etc. CIP-002-4 does not provide the appropriate link from CIP-002-4 to the other Standards. The question of what an entity is to do after this categorization is left to be answered, and until the stakeholders can see the entire scope of the CIP version 4 re-write, it is difficult, if not impossible, to pass judgment on this CIP-002-4 in isolation.
MWDSC	Recommend delaying effective date or concurrently developing CIP-003 through CIP-009 in order to determine if CIP-002 is reasonable. Also needs more implementation time or readiness assessments before making mandatory. Vague or unclear terms create opportunities for differing interpretations.
Empire	Consider: 1. Routable protocol or dial up accessibility as a criteria 2. A category for NO impact to the BES 3. Low impact with no communications = no controls 4. Evaluate events based on a single contingency 5. Readiness audits prior to mandatory dates 6. Financial impact vs. true BES impact prevention benefits 7. Approve CIP-002 though CIP-009 Version 4 as a package at the same time 8. Effective dates of CIP-002 same as CIP-003 through CIP-009 9. Performance based requirements

Organization	Question 13 Comments (Response page 25)
	10. No ambiguous language
BCTC	The guidance provides a process overview to an organization to do a risk assessment on assets and could better serve utilities on how to actually walk through a CCA process identification using the functional requirements listed in CIP002. Closer tying it back to CIP-002 would be of more value. An abbreviated start/example, from a Control Centre perspective, using a functionality approach, building off of CIP-002-4 is detailed below. *** To begin, each utility should determine, based on their registration status, which critical cyber asset functionality described in NERC CIP-002-1 R3.0 is applicable to them. For a control centre, critical operational functionality includes: Monitoring and control – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable supervisory control and data acquisition function (e.g. monitoring and control) of remote assets that support the reliable operation of the BES; Remedial Action Scheme – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the arming of the Remedial Action Scheme; Automatic Generation Control – the information system(s)/applications(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the automated functionality to support Automatic Generation Control; Real-time Power System Modeling – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the modeling to enable the reliable operation of the BES; and, Real-time Inter-Utility Data Exchange – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, network infrastructure), that enable reliable information transfer between neighboring utilities required to maintain the reliable operation of the BES To be considered a critical cyber asset the cyber asset must: 1. Be a system/application deployed in a real-time Production Environment; 2. The system/application must meet on or more of the following section criterion: a. Enable remote Monitoring and Control functionality (e.g. SCADA); b. Enable Remedial Action Scheme; c. Enable Automatic Generation Control; d. Enable Real-time Power System Modeling; and, e. Enable Real-time Inter Utility Data Exchange. 3. The system/application must use a routable protocol (e.g. Internet Protocol) to communicate between discrete electronic perimeters; or, the system/application must have a direct dial-up connection to a public network (e.g. Plain Old Telephone Line). From this point, the utility could develop the cyber systems inventory, as suggested in the drafts “step 1 & 2”, and verify if the systems enable the functional areas using a matrix

Organization	Question 13 Comments (Response page 25)
SWTC	Attachment 1 addresses the need to ensure that studies have been done, and can be documented to show, with approval by the Reliability Coordinator, that if a transmission subsystem is destroyed, degraded or rendered unavailable, it does not need impact the BES. (This is an oversimplification of what is stated; both planning and operations studies will be needed to document this.) There is similar wording for generation subsystems. The proposed CIP standard gives a definition for "Cyber Systems" and "BES Cyber Systems" but provides no guidance as to what those are or how they shall be designated by transmission and generator owners and operators. Instead, the standard launches into requirements for BES Subsystems. Neither does Attachment 1 address these. However, it could be construed that Attachment 2 addresses these as it discusses functions critical to the reliable operation of the BES and outlines aspects of control-type systems that utilize protection systems and relays. Attachment 1: How does this apply to a small(er) utility? and Who does it apply to? Additionally, I agree with the idea of subsystems is an unneeded step and adds confusion. However, I think one positive to the standard, is that the terms "critical assets," "critical cyber assets," and "cyber assets," go away. The standard offers no impact or applicability tier to BES elements/subsystems that are not critical to the BES. In other words, we don't have to worry about our assets being designated as "critical," but the onus is on us to determine, through discussion, evaluation and study, if they have an impact to the BES.
SCEG	It is imperative that the SDT provide guidance to the entities on the Security Controls (CIP-003-009) that will result from the 3 impact classification levels. It is unacceptable to ask the industry to vote to approve a standard without knowing the implications resulting from the standards directly associated with it. If some guidance on the resulting security controls coinciding with the classification level were provided, entities may feel more inclined to approve the standard.
Exelon	Exelon appreciates the effort of the SDT and recognizes the task assigned to the SDT is extremely difficult and challenging. As the SDT stated in the cover letter the revisions to CIP-002 will impact the entire suite of CIP standards that are currently in force, all without a clearly stated scope of applicability from the USNRC to U.S. nuclear plant generator owners/operators. Providing salient comments only on CIP-002 revision without understanding the full impact on the whole body of inter-related Regulations and Standards becomes problematic. We would encourage NERC to do whatever they can to add timeliness and clarity to this process. Section.5.1 (Physical Facilities) of the proposed standard discusses “not regulated by the NRC or the CNSC”, should include the following clarification “under 10 CFR 73.54”.. Balance of plant (BOP) scope is currently regulated by the NRC under 10 CFR 50.62, 10 CFR 50.63, and 10 CFR 50.65. Without the clarification, the CIP Standards would apply only to systems, structures and components (SSCs) not regulated under any NRC regulation. 10 CFR 73.54 is the regulation that applies specifically to cyber security. In addition the use of the term “facilities” throughout the CIP standards introduces an element of ambiguity and confusion when applicable entities are attempting to determine impacted systems, structures and components (SSC). We suggest that the SDT refrain from using the term “facilities” and begin introducing “systems, structures and components (SSC)” into the standards.
BPA Trans	Other Comments not already provided in response to earlier questions: First, it is difficult to address this Standard completely without understanding, at least at a high level, how it will interact with the revisions of the remaining CIP-003 through CIP-009 Standards. In particular: 1. Will the standards consider not only impact, but probability? The current standards do not allow any consideration of the probability

Organization	Question 13 Comments (Response page 25)
	that a particular vulnerability can and will be exploited. Instead, all threats are treated as being equally probable. As a result, considerable effort could be expended in protecting against threats that are extremely unlikely. 2. Will the entities have the ability to consider the level of risk after mitigation in determining whether to apply a requirement? Currently, the standards give no such flexibility, except for a limited range of Technical Feasibility Exceptions. As a result, strict compliance is required in almost all cases, even where compensating controls have reduced the level of risk to one commensurate or lower than the residual risk after applying the standard. 3. At a high level, what will be required for compliance at each BES Cyber System Impact Level? 4. Will there be any requirements levied on Low Impact BES Cyber Systems? As the impacts are presently defined, it would be hard to justify any such requirements. Low Impact BES Cyber Systems, by definition, can have no impact on the BES. However, the standard does not address that issue.
HQT	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.” to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline.
CCG	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot.
Allegheny Energy	• CIP-002, version 4 represents a radical departure from the previous versions. The transition from the approach in version 3 to version 4 is likely to be confusing and result in an abundance of new interpretations. We are concerned about the level of cyber assets that could now be interpreted to be in scope and not add to the reliability of the BES. • We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable. • This individual standard cannot be fully reviewed and commented on without reviewing the revisions that are being made to the related CIP-003 thru CIP-009 reliability standards. Further commenting and approval of this standard should be deferred until drafts of all the standards have been completed and made available for review. (For example what will be required of things categorized Low, Medium, High?) • The definition of "Engineering analysis" to get around the hard limits (1,000, 2,000) is too vague and re-assigns the responsibility for determining what is acceptable to the regions. This could create vastly differing interpretations among the various regions. At a minimum, more detail should be provided on what types of “engineering evaluations” for the GO and GOP would be acceptable to

Organization	Question 13 Comments (Response page 25)
	the Reliability Coordinator. • Because CIP-002 is so integral to the other reliability standards CIP-003 through CIP-009, this standard should not go into affect until "after the 1st day of the eighth quarter after regulatory approvals have been received for the revision of all CIP-002 through CIP-009". • The previous versions of CIP-002 specifically address only cyber devices that are accessible or can be accessible outside the physical location of the device. This was removed in the current draft. This should be should be put back in. Devices that are not externally accessible can adequately be protected, like any other piece of equipment, solely with physical security.
KCPL	No additional comments
MidAmerican	MidAmerican Energy Company supports modifying all the CIP standards to address the modifications in FERC directed Order 706. In response to FERC and industry concerns regarding identification of assets in CIP-002-1, a summary of revisions MidAmerican supports follows: (1) Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. (2) Change CIP-002-2 R2 to “reviewing the list of BES assets” instead of “developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required” as currently written in CIP-002-2. (3) Change CIP-002-2 R3 to use “the list of BES assets” instead of “the list of Critical Assets.” Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility. (4) CIP-002-4 cannot be implemented without the revised security controls . (5) Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunity to move forward with CIP-002. (6) Revise CIP-003 through CIP-009 within their existing framework as much as possible. Incorporate categorization discussed above, where applicable and meaningful. Provide more flexibility in the controls. Replace zero-defect quality prescriptions in the requirements, measures and violation severity levels with results based performance objectives. Explanation and details follow. Criticisms of the results from the existing standards are: not enough Critical Assets and Critical Cyber Assets were identified, and security controls are inflexible. The root causes of these unacceptable results are: (A) CIP-002-2 is not prescriptive enough. (B) CIP-003-2 through CIP-009-2 are too prescriptive, one-size fits all and the associated measures and violation severity levels prescribe zero-defect quality. MidAmerican submits that revisions within the existing framework of the standards will achieve the desired results more effectively and

Organization	Question 13 Comments (Response page 25)
	much faster than the significant framework changes proposed. (1) CIP-002-4 as proposed requires all BES all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards to be in CIP scope. It addresses the criticism that entities did not include enough assets. MidAmerican supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all owned BES assets (100 kV and above): transmission control centers that are subject to other existing NERC standards, transmission substations and generation resources. A very short list of objective, specific criteria for excluding an asset from CIP should be considered. For example, exclude wind farm generating units when the reliable operation of the grid doesn't yet rely on the wind blowing. For example, exclude small generating units under a certain MW nameplate unless the unit is in the primary black start unit because the other small units have minimal risk of contributing to success of a concerted, well-planned attack against multiple points. This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards. (2) Modify CIP-002-4 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in CIP-002-2. BES bright line criteria also eliminates the need for proposed CIP-002-4 R2 that addresses directly interconnected assets. All assets are held to the same bar across the industry. (3) Change CIP-002-2 R3 to use "the list of BES assets" instead of "the list of Critical Assets." Retain the concepts of and definitions for Cyber Asset and Critical Cyber Asset. Require inventory of Cyber Assets and Critical Cyber Assets for all BES Assets. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls. Categorization level determinations should be addressed in the security control standards. See (6) below. (4) CIP-002-4 cannot be implemented without the revised security controls . The implementation plan has to incorporate transition planning for Cyber Assets currently covered by CIP, if their security control requirements change under the revised standards. (5) Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it

Organization	Question 13 Comments (Response page 25)
	fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, MidAmerican recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) above, but moving the categorization aspects of CIP-002-4 into the development of security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. Where meaningful high, medium or low categories are identified, their criteria should be bright line. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might be on the list as one, but not the only, acceptable method to achieve the objective of low electronic authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161 kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. (6) Revise CIP-003 through CIP-009 within their existing framework as much as possible. MidAmerican supports the Standards Drafting Team's key principle to provide flexibility in applying equivalent security controls on the basis of compensating measures, cyber system characteristics and operating environment considerations. Analysis of the technical feasibility exceptions submitted in January 2010 should serve to underscore the importance of tailoring security controls between computers (desktops and servers) versus industrial controllers (relays and controllers) versus telecom gear (firewalls and switches). Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented; program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120); and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented; high-controls not implemented; moderate-reviews not completed; lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of

Organization	Question 13 Comments (Response page 25)
	concerted, well-planned attacks against multiple points.
CPG	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot. In addition, time and effort should be given to development and consideration of a "cyber first" approach. We appreciate that the proposed version seeks to protect the assets most critical to the bulk electric systems. However, the direction of this proposal may be missing some vulnerabilities and drawing some assets into scope that have little if any impact on reliability. For any approach taken, it is important to remain focused on reliability.
Santee Cooper	Other Comments not already provided in response to earlier questions: No one knows the elements and assets of a company better than the company itself. If we are considering changing this standard, it needs to be simple and absolutely clear. IF it is not clear, then it is left to the interpretation of regional entity and their audit teams. Without intimate knowledge of that company's system and assets, any room for interpretation would render an unjust burden on that company.
OGE	• Reliability Coordinator or Regional Reliability Assurer should provide a list of groupings of pre-approved engineering evaluations or other assessment methods. As stated, it is possible that the RC/RRA will be inundated with methods and could back-log in approvals, forcing RE's out of compliance. • Throughout the document, the "engineering evaluation or other assessment method" is referenced. The standard should designate that only the Responsible Entity is authorized to perform the engineering assessment to evaluate the BES Subsystem's impact. The method may be approved by the RC or RRA, but it should be applied by the Responsible Entity. • OGE proposes that the remaining standards be at least published for informal comments before the formal comment period on CIP-002-4. We need some idea of the controls SDT will be proposing in the following standards (what are now CIP-003 through CIP-009) before informed comments on proposed standard in CIP-002-4 are submitted. • Routable protocol or dial up accessible should be considered as method to limit the universe of BES cyber assets. • SDT should develop language that allows for the evaluate events based on single contingency • A Readiness audit prior to mandatory date should be performed without the threat of penalties. • SDT should allow for consideration of the "Financial impact" of risk mitigation when the threat is clearly inconsequential. • SDT should develop an awareness roadmap to help change the internal compliance culture as we migrate from Version 1,2,and 3 to Version 4. Many of the original concepts and terms are changing making the transition more difficult. • SDT should state how/why Version 4 increases BES security posture. • Overall we need greater clarity with the requirements to understand exactly how to meet the requirement. The terminology is vague and prone to misinterpretation.

Organization	Question 13 Comments (Response page 25)
	• Establish a "No Impact" category for those cyber assets that cannot be compromised by a cyber threat and that do not affect the bulk electric system? • Comments for CIP 002-4 should be requested at the same time as CIP 003-4 through CIP 009-4. • SDT should provide feed-back to these comments before final draft is submitted for comment in late Feb to avoid repeating many of the same comments during the 45 day formal comment period. • Define the "Bright line" and its purpose • Develop a detailed glossary of terms used in the drafting process and in the final requirements. It is very hard to provide the SDT with feedback without understanding the terminology. There is too much subjectively. • We need to be allowed to perform a risk assessment on the BES cyber device to determine if it could impact the electric asset(s) and in cases where the cyber risk below a certain threshold to the BES, then eliminate the device from consideration.
PPL Supply	Agree with EEI Comments. Also, Moving into the future, • We believe that standards development team should focus on the "What" of security control outcomes rather than the "How". • We suggest that the standards drafting team carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
NGRID	• National Grid recommends that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." to this version. • It is also advisable to have a FAQ/Guideline and move the examples into the FAQ/Guideline • National Grid believes that this standard partially represents the whole effort. Because this approach is so radically different it is critical that the SDT presents a complete package (CIP-002 – 009) for balloting.
MGE	An entity may have a blank list for High and Medium BES Impacts for attachment 1 but several items listed under attachment 2. Is it the intent of the SDT that if an item is listed on attachment 2, that it is a High or Medium BES Impact? Please clarify. We recommend that the SDT add a No BES Impact category along with High, Medium, and Low. If this Standard becomes enforceable, all cyber assets will fall into a Low, Medium, or High category. It is unreasonable to ask the industry to provide comments on this version of this standard without full clarification of High, Medium and Low and what the implications of those ratings are, without posting the proposed CIP-003 through CIP-009 at the same time. CIP-003 through CIP-009 may imply requirements unjustly. Please clarify. Upon reviewing this proposed Standard I kept asking myself "what threat are we guarding against"? Without knowing what the threat is, it is hard to defend or protect a BES cyber asset. One of the first rules in defending anything is to know the capabilities and limitations of your Aggressor.

Organization	Question 13 Comments (Response page 25)
FE	1. FE supports the expedited schedule for completing a new CIP suite of standards. We recognize the importance of this project and are committed to support completion by Year End 2010. 2. FE believes the industry should submit a complete suite of CIP-002 through CIP-009 standards. Trying to ballot CIP-002 ahead of the other standards presents problems for industry in regards to a complete understanding of expectations and impacts. Balloting CIP-002 ahead of the other standards presents coordination challenges in regards to an effective implementation plan. 3. FE encourages the team to reconsider the purpose of this standard as described above and believes the intent should be on identifying cyber vulnerabilities that could lead to High BES Impacts with appropriate H/M/L cyber asset controls based on the technology in use. A bright line of what will be considered High BES Impact threats should be the focus of Attachment 1. 4. FE does NOT support the work required in Attachment 2. The intended use of the information is not clear.
TECO	We support EEI's comments 1 – 8. In addition, we offer the following as input for consideration. TEC recommends reconsideration/removal of Shared Element as the definition of Element of the BES makes all of the Transmission system except radial transmission lines either a High or Medium. TEC would appreciate additional clarification of the terminology: "could hinder restoration to a normal condition." Routine restoration? Restoration following hurricanes, ice storms, etc? TEC has concerns that the list of assets required for compliance with the currently stated draft does not exist for any utility in the country (every span, protective relay, circuit breaker, etc. associated with a BES Subsystem). Creating such a list and keeping it up to date would require significant effort, documentation, coordination, etc. In addition, TEC strongly supports the following joint comments provided to the utility industry as it relates to the cyber first review of assets. We have incorporated those comments here: • Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective. • The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. • Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. • CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required.

Organization	Question 13 Comments (Response page 25)
	• The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… • The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below. Validity of the "Cyber First" Approach to Defining Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – system stability is the salient issue. • N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a coordinated multi-site attack, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on a perpetrator's ability to navigate across and between control system data networks in order to access multiple sites. • "Routable protocol" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented). • Thus, routable protocol networks are the correct object of cyber protection concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.] • At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means. • CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for all control cyber assets that communicate in common on a TCP/IP-based data network infrastructure; regardless of how big or small the grid operating site is in terms of electrical rating. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities relevant in practice to BES reliability. • If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is not for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not be imposed where cyber threat is not real. • Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the different Categories of cyber assets as characterized below. Identifying Specific Cyber Objects of Protection • Start by identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES

Organization	Question 13 Comments (Response page 25)
	Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement, execute, or support the Essential Functions. • Generally speaking, process and distributed control system elements at work at different types of grid operating site present three major cyber asset categories in terms of cyber risk exposure to the bulk electric system: o Category 1 (High): Control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate; these require the most rigorous cyber security controls and countermeasures because nefarious root capture of control system hosts represents the worst case scenario. o o Category 2 (Medium): "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use. Dial-up aside herein, these cyber assets require earnest cyber security controls and countermeasures, but nefarious root capture of same typically does not directly represent the same grid threat severity as do control system host computers themselves. o o Category 3 (Low): Cyber assets in use at all other operating sites that do not employ routable TCP/IP protocols to communicate. These should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc). • Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset identified above. More granular refinement of cyber security control and countermeasure Requirements will be necessary beyond the gross categorical illustration above, especially concerning Category 2. • Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not in terms of facility size/rating] • All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I. Advantages of the Recommended Approach • It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The subject is computers, not electricity. • This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's complimentary improvement, not do-over.
Snohomish	The Public Utility District No. 1 of Snohomish County ("District") support many aspects of the CIP 002 version draft. The focus on electric system impacts and the graduated risk levels should allow the electric industry to better focus resources on defending against the greatest risks to electric system reliability. However, we have a number of concerns with the MW thresholds that are used. Consistent with the many issues around the "bright line" voltage based definition used in the Bulk Electric System, the 1000/2000 MW/MVA thresholds do not accurately identify impact risk. "Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above."

Organization	Question 13 Comments (Response page 25)
	"Each Generation Subsystem with aggregate rated name-plate generation of 1000 MVA or more, not already included in section 1 above, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support." We prefer a more performance-based approach for both loss of load and generation - such as a utility or region cannot adversely impact neighboring systems. It is very likely that a wind or ice storm could impact 1,000 MW, by faulting key facilities. These types of conditions occur seasonally and should be classified as impacts to local customer service or Level of Service ("LOS"). On the other hand it is possible that facilities less than 1,000 MW may produce wide spread cascading. We suggest that the systems are tested on a system by system basis using TPL, and expanded TPL system assessments. If the facilities do not cause uncontrolled cascading and destroy equipment it should not be considered a reliability impact. However, a compromise may be to classify system categories by MW thresholds to determine the level of assessment that is needed to demonstrate level of BES impact. Such as less than 300 MW requires a powerflow assessment and 300-1,000 MW requires a powerflow and transient stability assessment, and greater than 1,000 MW requires expanded TPL assessments. This expanded assessment may include multiple simultaneous contingency evaluations that would simulate an orchestrated attack on various facilities. It should be noted that load loss should not be the threshold, cascading should be the threshold. The reason is we must benchmark the electric system performance against wind/ice storms and other natural and reoccurring events. If the system does not cascade out and the electric system (equipment is protected/isolated) load can be restored, we believe the system met its performance obligations. If the performance requirements are higher than this the electric industry will treat CIP risks at a much higher level than the seasonal risks that threaten our electric system on a continual basis. As noted above the District believes the engineering evaluations should be applicable to load areas levels as well as generation level (below). " …unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support." A preferred alternative: "…unless it has been determined not to produce wide spread cascading and is essential to the wide area [adversely impacts neighboring electric utilities] reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage, thermal, or frequency support. The District thanks the CIP-002 drafting team for the opportunity to comment.
CECD	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot.
MRO	We believe the intent of the current version of standard CIP-002-3 has a better security focus than the proposed version 4, and that the current version of standard CIP-002-3 should either be maintained, or combined with certain aspects of the version 4 proposal. The current version of standard CIP-002-3 identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to

Organization	Question 13 Comments (Response page 25)
	identify cyber systems critical to the operation of the BES sub-systems. It then goes one step further by differentiating between routable and non-routable connections to these cyber systems. We believe this differentiation is extremely important, since non-routable connections (or even better, eliminating connections wherever practical) are inherently more secure against, and limit potential damage from, remote attacks. This seems to be a straight forward and direct approach to securing the BES from cyber attack, and we do not see any reason to deviate, especially when you consider that version 4 appears to be migrating away from the core scope of protecting against remote cyber attacks. If the concern is too much latitude in the current version of standard CIP-002-3, then the new Identifying Critical Assets and Identifying Critical Cyber Assets guidelines should be rolled in to the current standard as core requirements instead of references, assuring that all entities identify critical assets under a similar, Engineering study based assessment. Completely replacing the existing standard with the entirely new approach of version 4 does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security, especially when the version 3 Identifying Critical Cyber Assets guideline is currently out for formal comment at the same time.
GTC	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards. 2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary? c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone

Organization	Question 13 Comments (Response page 25)
	fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could be lowered if certain protective criteria were met (encryption etc.). 5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas should produce a superior set of standards. 6. With respect to section 4.1 of the Standard, the second sentence, beginning "In situations where . . . ," should be deleted as unclear and unnecessary.
Tallahassee	TAL agrees with and supports the comments submitted by the APPA.
BGE	We believe that load management systems should be treated on par with generation resources. If requirements include generation units of a certain size, then load management systems of equal or greater value should also be included. According to Attachment 1, part 1.6, "Each Transmission Subsystem comprising the Cranking Paths" is considered "High BES Impact". Does the drafting team intend for switchable load-serving substations normally tapped from the Cranking Path to be included in the "Transmission Subsystem"? We note that in Attachment 1, part 1.1 (as well as in other parts of Attachment 1) that language is included that allows for engineering studies to be performed in order to demonstrate that a particular asset is not "High Impact". The standard states that the "engineering evaluation or other assessment method" must be approved by the Regional Reliability Assurer or Reliability Coordinator. We agree with the concept of allowing studies to show that an asset is not "High Impact". However, we believe the standard should address the criteria by which the RC or RRA would evaluate and approve a given evaluation. There should be more structure so that the RC or RRA decision to approve or reject a particular study is objective and not subjective. The prior version of CIP-002 considered two dimension of risk for critical cyber assets. The first risk considered impact, whether or not a

Organization	Question 13 Comments (Response page 25)
	cyber asset was associated with a critical BES asset. The second risk considered vulnerability by whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal the SDT has eliminated any consideration of the dimension of vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest that various categorization of vulnerability be designated in CIP-002 (High, Medium, Low or High, Low, No) and the sorting criteria be established in an appendix, similar to Attachment 1 of the current proposal that correspondingly deals with the dimension of impact. As well, understanding the design basis threat against which mitigation measures may be built is fundamental in creating an effective set of control measures. The threat potential basis should be clearly established. In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit CIP-002. After that time, a packaged set of CIP standards (including proposed revisions to CIP-003 to CIP-009 as they are currently known) should be presented for ballot.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question. Additionally, we suggest that the drafting team clarify that each BES Cyber System impact evaluation/assessment is limited to a single BES Cyber System and not multiple BES Cyber Systems.
FPL	We appreciate the hard work from the drafting team and support their efforts to ensure the reliability of the BES. The team has a difficult task in light of pressures from industry as well as Congress. We would like the drafting team to continue considering that the requirements drafted to secure the systems are appropriate to the risk. When considering BES subsystems impact, the level of risk should be commensurate with the amount of work needed to mitigate that risk. That is, in the case of low impact BES subsystems, we should consider the amount of work relative to the additional security relevant to the security of the BES. The focus should be kept on mitigating risks for remote and physical access with special attention on remote access vulnerabilities when there is connectivity.
TAPS	TAPS supports APPA's proposal submitted in response to this question that "the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment." To do otherwise would prevent stakeholders from voting in an informed manner.
Allegheny power	AP believes that a single package should be put forward that includes both the proposed standard for BES Cyber System Categorization, as well as the associated controls. This is the only way to allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of associated controls. AP agrees that there is value in identifying clear and straight forward bright line criteria for high, medium, and low impact BES assets. The bright line criteria should be subject to an approved engineering evaluation in the event that an entity owns or operates an asset that while meeting certain criteria, does not affect the BES to the level indicated by the bright line. AP believes that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility

Organization	Question 13 Comments (Response page 25)
	exceptions (TFEs). AP believes that the current written definitions for high and medium impact BES systems do not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations. Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. There are typically multiple alternatives for blackstart cranking paths, which can be a benefit to system restoration. The standard needs to specify the “primary” cranking path. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the “primary” cranking path should not be considered as high or medium impact BES Subsystems. AP would like to see controls revised to continue to have appropriate qualification based on use of routable protocols or networks that communicate outside the Electronic Security Perimeter.
FMPA	We applaud the effort to develop a uniform risk based assessment methodology for the industry. We believe that the direction is good, it is the details that we disagree with. We believe that a lot can be done to simplify and make less ambiguous, such as eliminating the concepts of functions and Subsystems and instead just focusing on worst case contingency / scenarios that can be caused by malicious use of a Cyber System and comparing those scenarios to the good start made in Appendix 1. There should be the ability to avoid doing any analyses or any comparison against criteria if an Entity already believes that one of the Cyber Systems they own has a High BES Impact specific to that Cyber System. The analyses and comparison against criteria should only apply to its Cyber Systems that the Entity believes are not High BES Impact. Independent 3rd Party Review FMPA is encouraged by the tiered approach to cyber-security proposed by the SDT, but is concerned that any bright-line metrics must be based on operationally sound regional parameters for BES planning and operations. We agree that use of entity-specific parameters concerning the classification of BES systems should be avoided, because this triggers the same difficult study issues that proved problematic during the identification of Critical Assets under CIP-002-1. However, while the need for entity-specific studies is reduced by using "bright line" regional metrics such as Contingency Reserves and IROLs that define normal and emergency operations, we cannot completely eliminate the need for entity-specific and sub-area studies, which may raise an issue concerning third party independent review of these entity-specific or sub-area studies. Many regional "fill-in-the-blank" standards raise similar issues. For example, the UFLS Standard Drafting Team, in its efforts to determine who should perform region-specific UFLS studies (e.g., to determine how much load to shed at what frequency and with what time delay), is considering a proposal to create a new Registered Entity called the “Regional Planning Coordinator Group.” Such a Regional Planning

Organization	Question 13 Comments (Response page 25)
	Coordinator Group could be useful to other standards as well, and could be the "right" entity to perform independent third party reviews. For these reasons, FMPA recommends that the CSO706 SDT propose to create a new Registered Entity called the "Regional Planning Coordinator Group." Similar in concept to a Reserve Sharing Group, all of the Planning Coordinators in a region would be required to become members of the Regional Planning Coordinator Group and would be required to perform and/or approve regional studies. The Regional Planning Coordinator Group would also be charged with the review and approval of studies by individual Registered Entities that propose to depart from the regional parameters and bright-line criteria approved under Attachment 1. The approach outlined above addresses regulatory directives that NERC standards not assign responsibility to comply with standards to the same entity that is responsible for assuring compliance with standards, while ensuring that the entity or entities responsible for performing regional studies have a wide-area perspective and the capability to fully assess the impacts of planning and operating studies. The Process for Industry Approval of CIP-002-4 Must be Synchronized with CIP-003-4 through CIP-009-4. We believe the industry the industry will find it difficult to reach consensus in support of CIP-002-4 and address all of the technical issues raised by this standard prior to its review of the associated security controls being developed standards CIP-003-4 through CIP-009-4. CIP-002 through CIP-009 cannot be taken one at a time. FMPA recommends that the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment. Under this revised development plan, the industry will have the opportunity to understand the whole suite of standards before they vote to give final approval to CIP-002-4. FMPA would support an industry-wide straw vote to garner conceptual approval of the next version of CIP-002-4 standard. Once so approved, the draft CIP-002-4 could be provided to the FERC and other regulatory bodies either on an informational basis or for conceptual approval. Such conceptual approval by industry and regulators would give the industry, the SDT, regulators and Congress greater confidence that NERC is making strides to complete this project expeditiously, while ensuring that the target end-state will be acceptable to stakeholders and government authorities.
Duke	We believe that the proposed CIP-002-4 is too prescriptive, and that a better approach would be to use the "Cyber First" approach. Also, we believe that it is essential that the other CIP standards should be revised and balloted in concert with CIP-002-4. The "Cyber First" approach should begin with identification of Cyber Systems that can impact BES reliability. The Cyber Systems should then be categorized based upon both their potential adverse impact and risk, and protection requirements established accordingly. For example Cyber Systems that are part of a routable protocol communication network are considered to have highest risk because of their potential "reach". But serial and dial-up communications could also be compromised and attacked in concert to impact multiple BES System facilities at once, so they must also receive appropriate consideration and protections. This approach to cyber security continues and builds upon work already done by the industry.
AESI	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has

Organization	Question 13 Comments (Response page 25)
	been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards. 2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary? c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could be lowered if certain protective criteria were met (encryption etc.).

Organization	Question 13 Comments (Response page 25)
	5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas should produce a superior set of standards. 6. With respect to section 4.1 of the Standard, the second sentence, beginning "In situations where . . . ," should be deleted as unclear and unnecessary.
IESO	In concurrence with the IRC we submit the same response as follows: It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. We are concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. As discussed in detail with regard to draft Requirement 1.2, we do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. In addition to the shortcomings detailed above, it should also be noted that evaluation of Asset Owners' Cyber Systems falls outside of the RC's expertise. The Commission expressed its concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are

Organization	Question 13 Comments (Response page 25)
	also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the registered entity perform the review. How can an RC review the BA it is also registered as? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this problem. It is not clear why R2 is needed.
Manitoba 2	Are the applicable entities the same for all the standards? Are all requirements applicable to all Applicable Entities?
OMPA	The CIP-002-4 approval process needs to be coordinated and in step with the controls portion of these standards; CIP-003-4 through CIP-009-4. It is difficult to accept the proposed methodology and concepts without the ability to see the entire set of requirements for a better understanding of what each impact level would require.
ATC	ATC appreciates all of the work and effort that the SDT has done to develop this standard, but believes that it represents only one piece of the whole effort. Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009 being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. ATC is not against this narrowing of the standard and believes that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. ATC has made a number of edits around this position and we hope that the SDT includes them in the next posting. ATC is offering up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical) 1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment 1 if they perform an engineering evaluation / assessment that satisfy Requirement 2. R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities

Organization	Question 13 Comments (Response page 25)
	territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) Second Options is covered in Questions X, X and X but is repeated here for greater clarity. 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…” 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by the responsible entity. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.)

Organization	Question 13 Comments (Response page 25)
	2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (ATC Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entity are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.9 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.10 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.11 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit. 1.12 Each Transmission Subsystem which contains Elements that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.13 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.14 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.16 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: ATC removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity.

Organization	Question 13 Comments (Response page 25)
	Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? As a Transmission only company ATC would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or generation) ATC believes strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.3 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.4 Each Transmission Subsystem which contains Elements that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 3) Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit as high. 4) Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 5) Entities that have multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 6) Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature

<table>
<tr><th>Organization</th><th>Question 13 Comments (Response page 25)</th></tr>
<tr><td></td><td>updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Please comment how a regional BES definition impacts the application of this standard. Meaning if an entity deems it has no material impact to the BES and that is "approved" then does that entity need to apply CIP-002.</td></tr>
</table>

Organization	Question 13 Comments (Response page 25)
	Specificity is needed in this standard as it is markedly different from general traditional engineering thought and entities need to ensure they are meeting NERC's intent, expectation, and are consistency applying this standard. In addition it minimizes interpretation. Consider the implementation plan to allow for a grace period as this requirement becomes mandatory or a mechanism that an entity can understand whether they've met the mark by the auditor before being penalized.
IMPA	IMPA would like the Cyber SDT to consider posting CIP-002-4 for second commenting at the same time they post CIP-003 through CIP-009 for first commenting. This will allow the industry to make comments on CIP-002-4 and know what CIP-003 through CIP-009 might have in them. For balloting purposes, IMPA would like to see all the CIP standards posted for balloting together at the same time (CIP-002-4 thru CIP-009-4). IMPA recommends a phase in period for implementing CIP-002-4 should be considered. (The first day of the eighth calendar quarter after applicable regulatory approval is the current effective date.) This Standard has the potential to be very costly in terms of manpower and expenses (especially since we don't know what impact the revised 003-009 Standards will have). A suggestion would be a Responsible Entity has to have 50% of their assets evaluated after 8 quarters, 75% after 10 quarters, and 100% after 12 quarters.
ERCOT	• ERCOT ISO supports Midwest ISO Comments. • It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. • Title – The title should change to state "BES Cyber System Identification and Categorization" since the Purpose explicitly says "to identify" BES Cyber Systems. Also, the verbiage of the 3 Requirements indicates that identification is "assumed" when categorizing. • Section 5.1 Physical Facilities – The use of "BES facilities" is different and inconsistent with "BES Facilities" used in the definition for BES Subsystem. Recommend "BES Facilities" be added to the Definition of Terms and used consistently. The language appears to be an incomplete thought. The language only addressed nuclear facilities. • Effective Date – The effective date should be consistent with the regulatory approval of CIP-003-4 through CIP-009-4. The requirements and terminology across the standards should be consistent and aligned. If this cannot be accomplished, a cross reference of prior terms to new terms should be addressed. (i.e.: critical asset to the new term, critical cyber asset to the new term, non-critical cyber asset to the new term, etc.) • It appears that the new standard relieves Responsible Entities from a periodic review and reaffirmation of their lists when there are no changes to the assets. • An implementation schedule should be addressed for the timeline to implement controls where assets have been reclassified due to the adoption of this new approach. If the current Implementation Plan for New Identified Critical Cyber Assets and Newly Registered Entities is intended for use to determine these timelines, it should be so stated. • Figures 5, 6, & 7 in the concept paper mention a specific vendor's product (PI). While that document is not under review it should be noted that this document should be corrected with a generalized term such as data historian.

Organization	Question 13 Comments (Response page 25)
	Midwest ISO Comments: • In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. • It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. • We are also concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. • The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. • We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also

Organization	Question 13 Comments (Response page 25)
	registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA if it is also registered as the BA? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation. • We are concerned about the addition of the function entity Reliability Assurer. While it was added to the most recent Functional Model, we believe it is premature to begin using this entity. While many believe that NERC and the Regional Entities are ultimately the Reliability Assurer, the function model is not clear this is the case. Furthermore, the Functional Model Working Group purposely drafting the Functional Model in a way so that it does not have to be the Regional Entities and/or NERC. Does the drafting team have a vision of whom the Reliability Assurer is? It has not been shared and we believe the drafting team needs to make clear whom they believe serves this role before it is added as new functional entity. Has this addition been coordinated with NERC certification and registry staff whom will have to register and certify this entity?
IRC	It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. We are concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. As discussed in detail with regard to draft Requirement 1.2, we do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. In addition to the shortcomings detailed above, it should also be noted that evaluation of Asset Owners' Cyber Systems falls outside of the RC's expertise. The

Organization	Question 13 Comments (Response page 25)
	Commission expressed its concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the registered entity perform the review. How can an RC review the BA it is also registered as? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this problem. It is not clear why R2 is needed.
PEPCO	1. We support NERC's efforts to develop a complete revised set of CIP standards in 2010, with a plan to file the new set of Standards with FERC in early 2011. We recognized the importance of this activity and are committed to this effort. We believe that the new CIP standards development project is one of the most important activities facing both NERC and the industry in 2010. 2. We believe that CIP-002 -4 should be developed. Balloted, and submitted as a single package with CIP-003-4 through CIP-009-4 NERC. This will allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. 3. We believe that the industry should move to a less administrative burdensome process and more of a performance based effort by using the proposed modified cyber approach as previously discussed. The proposed approach would not require classification or identification of big iron, would limit the focus to defined in-scope cyber control systems, and would apply the appropriate security measures/requirements based on specific criteria (e.g. operating platform, connectivity of the asset, span of control of the cyber asset's impact). 4. We believe that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility exceptions (TFEs).
NEI	A) Need to specify screening criteria. B) CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. Balloting CIP-002 ahead of the other standards presents coordination challenges in regards to an effective implementation plan. C) The process for notification and request for comment needs improvement. Personnel who are site Cyber Security personnel were not aware until after NEI notification. The materials were also not easy to find on the NERC website. D) The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. E) Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based

Organization	Question 13 Comments (Response page 25)
	upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. F) The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… G) Alternative Top-down argument for defining the correct CIP Standards' Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue. • N-1 engineering also dictates that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on the perpetrator's ability to *navigate* across and between control system data networks to *access* multiple sites. H) Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective. I) The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. J) Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. Furthermore, CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. K) The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… L) The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below. <u>Validity of the "Cyber First" Approach to Defining CIP Standards' Scope of Applicability</u> • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue. • N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on a perpetrator's ability to *navigate* across and between control system data

Organization	Question 13 Comments (Response page 25)

	networks in order to *access* multiple sites.
	• "Routable *protocol*" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented).
	• Thus, routable protocol networks are the *correct object of cyber protection* concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.]
	• At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that *do not* run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence *in practice do not pose a salient threat* to BES reliability *through cyber means*.
	• Process and distributed control system elements at work in different types of grid operating sites present three major cyber asset categories in terms of *risk exposure*:
	  o Category 1 (High): control/data/operations centers employing TCP/IP;
	  o Category 2 (Medium): field operating assets employing TCP/IP (substations, dams, generators, etc.); and, dial-up regardless of other communications protocols also in use;
	  o Category 3 (Low): all other sites served by cyber control system elements that do not employ routable TCP/IP protocol communications.
	• CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for *all control cyber assets that communicate in common* on a TCP/IP-based data network infrastructure; *regardless of how big or small the grid operating site is in terms of electrical rating*. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities relevant in practice to BES reliability.
	• If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is *not* for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not be imposed where cyber threat is not real.
	• Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the above Categories, as follows:
	<u>Identifying Specific Cyber Objects of Protection</u>
	• Identify the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement and execute the Essential Functions.

Organization	Question 13 Comments (Response page 25)

	• Categorize the specific cyber assets (above) in use into the following subsets:
	  o Category 1 cyber assets using TCP/IP to communicate
	  o Category 2 cyber assets using TCP/IP to communicate; and any others which employ dial-up communications, regardless of what other type of protocol the cyber asset may use to communicate elsewhere.
	  o Remaining cyber assets represent Category 3, and should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc.).
	• Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset, as identified above.
	• Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not in terms of facility size/rating]
	• All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I.
	<u>Advantages of the Recommended Approach</u>
	• It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The subject is computers, not electricity.
	• This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's complimentary improvement, not do-over.
	• It results in application of cyber defenses appropriate to true risk, and does not require expense and effort securing assets that do not pose a genuine vulnerability/threat.
	• It provides Responsible Entities the autonomy to manage gradual replacement of antiquated data networking in favor of high performance TCP/IP networking that demands more rigorous cyber security controls and countermeasures.
	• It provides the industry time to evaluate and consider the impact of Smart Grid and NASPI on security controls/countermeasure needs prior to upgrading control systems networking.
	M) NEI encourages the team to reconsider the purpose of this standard as described above and believes the intent should be on identifying cyber vulnerabilities that could lead to High BES Impacts with appropriate H/M/L cyber asset controls based on the technology in use. A bright line of what will be considered High BES Impact threats should be the focus of Attachment 1.
	N) NEI does NOT support the work required in Attachment 2. The intended use of the information is not clear.

Executive Summary of Consideration of Comments on CIP-002-4 – Categorization of Cyber Systems

A first draft of CIP-002-4 was posted in December 2009 for an informal comment period of 45 days ending in February 2010. The industry responded to the posting with more than 500 pages of comments from more than 90 entities. The following is a summary of comments received and the response, where applicable, from the Standards Drafting Team (SDT). Note that the drafting team made so many changes to the standard based on stakeholder comments that the team is proposing the revised standard be given a new number, "CIP-010."

1. **Definitions.** Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

   Summary Response: *A number of respondents' comments indicated some confusion between the definitions of Cyber System and BES Cyber System. Many also commented that the definition of Cyber System was too broad. The SDT considered these comments, has removed the definition of Cyber System since it is not referenced in the standard, and has modified the definition of BES Cyber System to include some of the concepts in the original definition of Cyber System into a single definition for BES Cyber System.*

   Respondents also commented on the definitions of Subsystems (BES, Generation and Transmission), cited vagueness and suggested the use of terms already defined in the glossary and in wide use in the industry. The SDT reviewed the comments and agreed that the use of terms already defined and widely used in the industry will serve the same purpose. The definitions for Subsystems have been removed and the references in the standard use terms already defined in the NERC Glossary or in wide use by the industry and any additional clarifying terms in the standard where "subsystems" were previously used.

   Many respondents commented that the definition of Control Center needed more specific bounds. The SDT has modified the definition to add more specificity.

   There were many comments on the need for definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1. The SDT reviewed them and has removed these definitions.

   Many also commented on the absence of a "No Impact" category. It is the SDT's opinion that the definition of BES Cyber Systems effectively removes Cyber Systems with no impact from the scope, and that a BES Cyber System has some level of impact, by definition.

2. The **Purpose** of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems

have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Summary Response: *There were a number of comments related to the absence of consideration for how BES cyber systems are connected in the categorization process. After much discussion, the SDT agrees that network connectivity should be a consideration, but that it is more appropriate to be considered in the drafting of requirements or controls that apply to categorized BES Cyber Systems or their components.*

There were comments that addressed the approach where inheritance from the BES Subsystem Impact level would result on the same level of impact for all BES Cyber Systems associated with the subsystem. The SDT has made substantial changes to the draft to allow entities to use any method to identify BES Cyber Systems (i.e. to start with an inventory of all BES Cyber Systems, or to start with BES Facilities and the BES Cyber Systems supporting their real-time operations), as long as all BES Cyber Systems are identified.

Many respondents noted in their comments that they can only evaluate the purpose if the requirements and controls are posted together. The SDT has considered these comments and is posting the new draft together with drafts of the requirements or controls.

The ***Purpose*** *has been redrafted to reflect these considerations.*

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversely impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Summary Response: *Of the 93 responses for this question, 49 preferred the method in the initial posting, 37 preferred the alternative method, and 7 did not have a preference. Many respondents commented that simplified criteria were needed. Some respondents noted that the standard should provide flexibility to use either approach. One entity noted that both alternatives must be executed in a comprehensive approach. Another entity commented on using CIP-002-3 as a base, expanding to all BES assets and applying the list of asset types in R1.2. Eight entities suggested using an approach based mainly on connectivity and secondarily on control centers and others. Some entities noted that a preference cannot be made in the absence of the controls. One entity proposed a hybrid approach, using a BES impact approach to filter out low impact BES Subsystems, then switching to a BES Cyber System based approach and classify based on the span of control of these BES Cyber Systems. Others cited the matrix approach described in the concept paper.*

The SDT considered all comments and has made substantial changes to the requirements in CIP-002-4 (now CIP-010-1) to allow an entity to use any approach to reach the goal of the final

categorization of BES Cyber Systems. The new requirements are drafted with more focus on the objective and desired outcome, rather than on the methodology or process.

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems.

1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."

Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Summary Response: *Of the total of 93 respondents, many commented again on the need to know the impact of controls. A number of respondents commented on the requirement for the Reliability Coordinator (RC) to approve engineering analyses: these commenters noted that RCs should be removed from these criteria. Some suggested that the Planning Coordinator is better suited for that role. Others commented that criteria for evaluation of engineering analyses were needed and that approved engineering analysis methodologies should be published. Some suggestions were made to specify a blanket option for engineering analyses to all criteria.*

There were a number of comments on the requirement for update, many on the amount of time specified before a change in the electric system is reflected. There were comments about the vagueness of the concept of BES Subsystems, and about questions of joint ownership, since the requirements focus on asset ownership. There were also comments on the open ended nature of the word "any" in the requirement.

The SDT considered these comments and has made substantial changes to the requirements. With a direct BES Cyber System to criteria for impact approach, the traditional use of BES impact engineering analyses becomes unnecessary for the evaluation of BES Cyber Systems, nor does any widely used methodology exist for that purpose. The criteria is now be based on bright lines and the impact categorization based on that of the BES Cyber Systems on the functions provided by BES Facilities.

The requirement for reviewing the categorization is now a separate requirement and based on changes in the BES Facilities that the entity owns or operates. The update period has also been extended to 60 days.

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)
2.2 The Responsible Entity name
2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

Summary Response: *The SDT thanks all respondents who commented on this requirement. In consideration of the overall comments received, the more direct statement of the impact categorization of BES Cyber System makes the requirement for notification unnecessary. This requirement no longer exists in the revised draft of CIP-002-4 (now CIP-010-1).*

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

Summary Response: *Respondents commented that attachment 2 (Reliability Functions) was overly broad and open-ended, and that the focus should be on real-time systems. Many commented on the potential absence of correlation between the impact level of the BES Subsystem and the impact of the associated BES Cyber Systems on the functions. Others commented that the categorization methodology should be similar to that described in the*

concept paper. Some noted that risk should be considered, not just impact: many cited connectivity as a factor. Some commented that there should be a No Impact category.

In consideration of these comments, the SDT has made substantial changes to the requirements. The categorization requirement is no longer based on an inherited categorization based on the impact level of the BES Subsystem, but each BES Cyber System is categorized based on its impact on BES Facilities which perform reliability functions. The scope has been clarified: BES Cyber Systems in scope are those which impact real-time operations of the BES.

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Summary Response: *Many respondents found it excessive for all requirements to have a High Violation Risk Factor. Some commented on the difficulty of assessing what was missed in the categorized BES Subsystems or Cyber Systems. Some commenters noted that requirements must be made clearer to properly make the assessment of the VSLs. There were many specific suggestions for changes to the wording in the VSLs.*

The SDT has redrafted the VSLs based on the substantially changed requirements in the new draft and on existing VSL drafting guidelines. VRFs have been assigned to the redrafted requirements.

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria?

Summary Response: *Many respondents commented on the need to have the draft of requirements and controls available for review in order to comment. Commenters also wrote that criteria could be boiled down to two metric: supply/demand mismatch and exceeding IROLs. Many comments questioned the basis of the bright line thresholds in the criteria. A number of comments questioned the use of gross nameplate values for evaluation of generation capability and cited the MOD-024 for rating of generation capabilities. One commenter stated that exceeding an IROL within the timeframe allowed by standards should not be High Impact. Commenters also questioned the use of the phrase "…leaving the station". Some entities aked whether Distribution Facilities supporting restoration and UFLS were in scope.*

In formulating the thresholds and bright-line criteria, the SDT used many sources, such as the threshold in the NERC Event Analysis categories, and various thresholds used in existing standards.

The criteria are now used to categorize BES Cyber Systems based on their impact on the functions performed by BES Facilities. In consideration of comments, the SDT has revised, consolidated and removed various criteria in the former attachment 1. Most notably, the bright line criteria for generation are now based on defined terms in the NERC Glossary and used in standards MOD-024 and MOD-025. Criteria duplicative with IROLs have been restructured as options where IROLs are not used, and other criteria have been clarified and corrected where

required. Periodic and time parameters have been added where there may be multiple criteria thresholds within a given time.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

Summary Response: *The vast majority of respondents had no suggested criteria for these entities. In fact, most felt that these entities should not be included as responsible entities in this standard. Those that felt that they should be included added that it depended on whether they had BES Cyber Systems. Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)*

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

Summary Response: *The only respondents that felt these entities should be included said that NERCNet was probably the only concern. Several felt that even NERCNet would not affect the BES.*

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?

Summary Response: *Most respondents felt that the Reliability Assurer could be excluded (pointing to the fact that the RA is not included in the NERC Glossary and confusion over how compliance for NERC and Regional Entities could be measured). Results for the Distribution Provider (DP) were mixed. Some felt that the DP could be excluded, since they did not involve facilities >= 100kV. Some felt that the DP should be substituted for the LSE. Some were unsure how load shedding and Smart Grid would affect this standard. Some were very opposed, feeling this opened distribution up to FERC regulation.*

The SDT agrees that the Reliability Assurer can be excluded, especially now that there is no requirement that directly references Reliability Assurers. However, there are many criteria that can direct affect Distribution Providers, especially when considering the NERC registration criteria for Distribution Providers. Such attachment 1 criteria for Protection Systems and UFLS can directly affect DP's that have such systems that are relevant for BES reliability. Registration criteria also point out that DPs that also satisfy Load Serving Entity registration criteria should register as LSEs. The SDT has included DPs in the list of applicable Responsible Entities.

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

Summary Response: *Many respondents reiterated that the focus for these functions should be cyber systems that support real-time operations. Many found issue with the "include, but are not limited to" section of the functions. Others commented that attachment 2 is confusing and*

should be eliminated. Comments were made about unintended reliability effects, citing blackstart units as high impact, and therefore could result in reduction of these units. Commenters also wrote that the examples should be moved to a guidance document. One commenter noted that attachment 2 has a wider application and does not belong in a CIP standard.

The SDT has clarified the scope of the functions and removed all the examples. The former attachment 2 is a necessary attachment to define the scope for BES Cyber Systems and the functions they support.

Consideration of Comments on Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4

The Cyber Security Order 706 Standard Drafting Team (CSO 706 SDT) thanks all those who submitted comments on the draft CIP-002-4 standard. This standard was posted for a 45-day informal public comment period from December 29, 2009 through February 12, 2010. Stakeholders were asked to provide feedback on the standard through a special electronic comment form. There were 107 sets of comments, including comments from more than 200 different people from approximately 90 companies representing all 10 of the Industry Segments in the Registered Ballot Body as shown in the table on the following pages.

In this document, the CSO 706 SDT's summary consideration of all comments provided in response to each question is provided in text highlighted in blue immediately following each question. The original submittals can be viewed at the following site:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Based on stakeholder comments, the standard (now CIP-010-1) allows entities to use any method to identify BES Cyber Systems (i.e. to start with an inventory of all BES Cyber Systems, or to start with BES Facilities and the BES Cyber Systems supporting their real-time operations), as long as all BES Cyber Systems are identified. Significant changes include:

Definitions:

- Removed the definition of BES Subsystem, Generation Subsystem and Transmission Subsystem as stakeholders indicated these terms are understood and don't need to be defined
- Removed the definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1
- Removed the definition of Cyber System and modified the definition of BES Cyber System to include some of the concepts in the original definition of Cyber System into a single definition for BES Cyber System
- Modified the definition of Control Center to add more specificity

Purpose:

- Modified the purpose statement to clarify that the application of cyber security requirements is designed to be proportional to the relationship between the BES Cyber System and reliability of the BES.

Applicability:

- Added the Distribution Provider, but not the Reliability Assurer and did not delete any of the already identified functional entities.

Requirements:

- Requirement R1: Modified the requirement to allow an entity to use any approach to reach the goal of the final categorization of BES Cyber Systems.
    - Converted Requirement R1, Part 1.1 for updating the categorization of BES Subystems into a separate requirement based on changes in the BES

Facilities that the entity owns or operates. The update period was extended from 30 to 60 days.

  - Eliminated Requirement R1, Part 1.2 requiring use of an engineering evaluation or other assessment method approved by the Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems

- Requirement R2: Eliminated the requirement for owners of specific Generation Subsystems to share BES impact categorization information to owners of directly connected Transmission Subsystems
- Requirement R3: The categorization requirement is no longer based on an inherited categorization based on the impact level of the BES Subsystem, but each BES Cyber System is categorized based on its impact on BES Facilities which perform reliability functions. The scope has been clarified: BES Cyber Systems in scope are those which impact real-time operations of the BES.

VRFs and VSLs:

- As each of the requirements underwent significant modification, the drafting team developed new VRFs and VSLs.

Attachment 1:

- The criteria in the attachment are now used to categorize BES Cyber Systems based on their impact on the functions performed by BES Facilities. The SDT revised, consolidated and removed various criteria in the former Attachment 1. Most notably, the bright line criteria for generation are now based on defined terms in the NERC Glossary and used in standards MOD-024 and MOD-025. Criteria duplicative with IROLs have been restructured as options where IROLs are not used, and other criteria have been clarified and corrected where required. Periodic and time parameters have been added where there may be multiple criteria thresholds within a given time.

Attachment 2:

- Modified the scope of the functions and removed all the examples. The former Attachment 2 is a necessary attachment to define the scope for BES Cyber Systems and the functions they support.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification. 15

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data. 15

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. 36

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy. 52

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System. 65

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System. 80

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: 93

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable: 111

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could: 137

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not: 156

2. The Purpose of draft CIP-002-4 states, “To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES.” Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement. 173

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber

Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method. 191

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. 210

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem: 245

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows: 260

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs. 278

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria? 293

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?333

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities? 345

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities? 351

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions? 362

13. Do you have any other comments to improve the draft standard? 374

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Individual	Jennifer Bullock	Progress Energy	X		X		X	X				
2.	Group	Jack Cashin	EPSA					X					
3.	Individual	Greg Mason	Dynegy, Inc					X					
4.	Individual	G. Mark Cole	Georgia System Operations Corporation & Oglethorpe Power Corporation			X	X	X					
5.	Individual	Ernie Hayden	Private Citizen										
6.	Individual	Randy Schimka	San Diego Gas and Electric Co	X		X		X					
7.	Group	Allen Mosher	American Public Power Association										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Eric Olson	Transmission Agency of Northern California	WECC	1
2.	Scott Miller	Municipal Electric Authority of Georgia (MEAG)	SERC	1, 3, 5
3.	Frank Gaffney	Florida Municipal Power Agency (FMPA)	FRCC	1, 3, 5
4.	Virginia Cook	JEA	FRCC	1, 3, 5
5.	Jonathan Appelbaum	Long Island Power Authority	NPCC	1, 3
6.	David Godfrey	Texas Municipal Power Agency (TMPA)	ERCOT	1, 5
7.	John Allen	City Utilities of Springfield, Missouri	SPP	1, 3, 5

8.	Individual	Joylyn Stover	Consumers Energy			X	X	X					
9.	Group	Guy Zito	Northeast Power Coordinating Council										X

Additional Member	Additional Organization	Region	Segment Selection

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		1. Alan Adamson	New York State Reliability Council, LLC NPCC 10										
		2. Gerry Dunbar	Northeast Power Coordianting Council NPCC 10										
		3. Gregory Campoli	New York Independent System Operator NPCC 2										
		4. Roger Champagne	Hydro-Quebec TransEnergie NPCC 2										
		5. Kurtis Chong	Independent Electricity System Operator NPCC 2										
		6. Sylvain Clermont	Hydro-Quebec TransEnergie NPCC 1										
		7. Chris de Graffenried	Consolidated Edison Co. of New York, Inc. NPCC 1										
		8. Lee Pedowicz	Northeast Power Coordinating Council NPCC 10										
		9. Mike Garton	Dominion Resources Services, Inc. NPCC 5										
		10. Brian L. Gooder	Ontario Power Generation Incorporated NPCC 5										
		11. Kathleen Goodman	ISO - New England NPCC 2										
		12. David Kiguel	Hydro One Networks Inc. NPCC 1										
		13. Michael R. Lombardi	Northeast Utilities NPCC 1										
		14. Randy MacDonald	New Brunswick System Operator NPCC 2										
		15. Greg Mason	Dynegy Generation NPCC 5										
		16. Bruce Metruck	New York Power Authority NPCC 6										
		17. Chris Orzel	FPL Energy/NextEra Energy NPCC 5										
		18. Robert Pellegrini	The United Illuminating Company NPCC 1										
		19. Saurabh Saksena	National Grid NPCC 1										
		20. Michael Schiavone	National Grid NPCC 1										
		21. Peter Yost	Consolidated Edison Co. of New York, Inc. 3										
10.	Group	Tracey Stewart	Southwestern Power Administration	X									
11.	Individual	Shawn Barrett	Michigan Public Power Agency					X					
12.	Individual	Steve Alexanderson	Central Lincoln			X							
13.	Individual	Jian Zhang	TransAlta					X					
14.	Group	Michael Assante	NERC										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Scott Mix	NERC CIP	NA - Not Applicable	
2.	Gerry Adamski	NERC Standards	NA - Not Applicable	
3.	Tim Roxey	NERC CIP	NA - Not Applicable	
4.	Ralph Anderson	NERC CIP	NA - Not Applicable	

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		5. Roger Lampila	NERC Compliance NA - Not Applicable										
		6. Tom Hofstetter	NERC Compliance NA - Not Applicable										
		7. Todd Thompson	NERC Compliance Investigations NA - Not Applicable										
15.	Group	Ruth Blevins	Dominon Resources Services, Inc.	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Robert S. Wright	Operations Center	SERC	3
2.	Carl J. Eng	Elec Tran Sys Operations	SERC	1
3.	Joseph R. Finnegan	Elec Tran Sys Operations	SERC	1
4.	Jeff Heffelman	F&H Sys Operations	SERC	5
5.	Matthew Woodzell	F&H Regulatory Compliance	SERC	5
6.	Michael Gildea	Elec Market Policy	NA - Not Applicable	NA
7.	Marvin Walker	IT Support - ET Sys Operations	SERC	1
8.	Steve Edwards	Elec Tran Reliability	SERC	1
9.	Perry Esposito	F&H Engineering	SERC	5
10.	Chip Humphrey	F&H Merchant Operations	RFC	5
11.	Fatima Ahmed	F&H Merchant Operations	RFC	5
12.	Connie Lowe	F&H Market Ops Center	SERC	5
13.	Marc Gaudette	IT Risk Management	MRO	5
14.	Charles Bonner	F&H Energy Supply	SERC	5
15.	John Calder	Elec Tran Compliance	SERC	1
16.	Vern Colbert	Trans Systems Oper	SERC	1
17.	John Loftis	Elec Tran Compliance	SERC	1
18.	Tim Morrissey	Merchant Operations Support	NPCC	5
19.	Art Bevilacqua	DENE Salem Support	NPCC	5
20.	Dennis Sollars	IT Compliance	NA - Not Applicable	NA
21.	Louis Slade	Electric Market Policy	SERC	6
22.	Mike Garton	Electric Market Policy	MRO	5
23.	Randy Reynolds	Elec Tran Substation Eng	SERC	1
24.	George Wood	Elec Tran Substation Ops	SERC	1
25.	Ronnie Bailey	Elec Tran Planning	SERC	1

16.	Group	Matt Luallen	Encari								X		

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		Additional Member / **Additional Organization** / **Region** / **Segment Selection**											
		1. Mark Simon / Encari / NA - Not Applicable / 8											
		2. Peter Brown / Encari / NA - Not Applicable / 8											
		3. Steve Hamburg / Encari / NA - Not Applicable / 8											
		4. Lenny Mansell / Encari / NA - Not Applicable / 8											
		5. Justin Harvey / Encari / NA - Not Applicable / 8											
17.	Individual	Karl Bryan	US Army Corps of Engineers, Northwestern Division	X				X					
18.	Individual	Patrick Farrell	Southern California Edison Company	X		X		X	X				
19.	Individual	Martin Bauer	US Bureau of Reclamation					X					
20.	Group	Ron Blume	Dyonyx										
21.	Individual	Thomas E Washburn	FMPP		X								
22.	Group	Jason Marshall	Midwest ISO		X								
		Additional Member / **Additional Organization** / **Region** / **Segment Selection**											
		1. Greg Mason / Dynegy / NPCC / 5											
		2. John Alberts / Wolverine Power Cooperative / RFC / 1											
		3. Barb Kedrowski / We Energies / RFC / 3, 4, 5											
		4. Lee Kittelson / Otter Tail Power / MRO / 1											
		5. Bill Hutchison / SIPC / SERC / 1, 3, 4, 5											
		6. Michael Ayotte / ITC / RFC / 1											
		7. Randi k. Woodward / Minnesota Power (ALLETE, Inc.) / MRO / 1											
		8. Joe Knight / Great River Energy / MRO / 1, 3, 5, 6											
23.	Individual	Bo Jones	Westar Energy	X		X		X	X				
24.	Individual	Green Country Energy	Green Country Energy					X					
25.	Individual	Jerome (Jerry) Murray	Oregon PUC Safety Reliability Security Staff									X	
26.	Individual	Kevin Calhoun	NB Power Generation					X					
27.	Individual	Tony Weekes	MB Hydro (Manitoba 1)	X									
28.	Individual	John Alberts	Wolverine Power Supply Cooperative, Inc	X		X		X	X				
29.	Individual	Mike McClain	Portland General Electric (Portland GE)	X		X		X	X				
30.	Group	Chris Klemm	Public Service Enterprise Group Companies (PSEG)	X		X		X	X				
		Additional Member / **Additional Organization** / **Region** / **Segment Selection**											

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		1. Robert N Green	PSE&G / RFC / 1, 3										
		2. David Murray	PSEG Fossil, LLC / RFC / 5										
		3. Clint Bogan	PSEG Power CT, LLC / NPCC / 5										
		4. Dominic DiBari	Odessa Power Partners, LLC / ERCOT / 5										
		5. James Hebson	PSEG Energy Resources and Trade, LLC / RFC / 6										
31.	Individual	William Lucas	Wisconsin Electric Power Company (WE-Energies)			X		X					
32.	Individual	Mike Hendrix	Idaho Power Company	X		X		X					
33.	Group	Stephen Mizelle	Southern Company Services, Inc. (SOCO)	X									
		Additional Member	**Additional Organization** / **Region** / **Segment Selection**										
		1. Marc Butts	Southern Company transmission / SERC / 1										
34.	Group	Mark Stefaniak	Detroit Edison (DTE)			X		X					
		Additional Member	**Additional Organization** / **Region** / **Segment Selection**										
		1. Mark Stefaniak	Detroit Edison / RFC / 3, 5										
		2. Chris Plensdorf	Detroit Edison / RFC / 3, 5										
		3. Brian Schulte	Detroit Edison / RFC / 3, 5										
		4. Tom Kopera	Detroit Edison / RFC / 3, 5										
35.	Individual	James H. Sorrels, Jr	American Electric Power (AEP)	X		X		X	X				
36.	Individual	John Falsey	Edison Mission Marketing and Trading					X					
37.	Individual	Rob Burt	Capital Power Corporation					X					
38.	Individual	Roger Fradenburgh	Network & Security Technologies Inc (NS&T)								X		
39.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X							
40.	Group	Brent Ingebrigtson	E ON U.S,	X		X		X	X				
41.	Individual	Kevin Emery	Carthage Water and Electric Plant			X							
42.	Individual	Louise McCarren	Western Electricity Coordinating Council										X
43.	Individual	Dave Norton	Entergy	X		X		X					
44.	Individual	John Brockhan	CenterPoint Energy Houston Electric	X		x							
45.	Individual	Don Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition (CA Cogen)										
46.	Individual	Dave Sutherland	LCRA Transmission Services Corporation	X									
47.	Individual	Linda Campbell	FRCC										X

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
48.	Individual	Tim Conway	Northern Indiana Public Service Company (NIPSCO)	X		X		X	X				
49.	Individual	Christopher L. de Graffernied, Sr.	on behalf of Consolidated Edison Co. of NY, Inc. and Orange & Rockland Utilities (ConEd)	X		X		X	X				
50.	Group	David Batz	EEI										
51.	Individual	Edward Bedder	Orange and Rockland Utilities Inc (O&R)	X		X							
52.	Individual	Kenneth A Goldsmith	Alliant Energy				X						
53.	Individual	Kirt Shah	Ameren	X		X		X	X				
54.	Individual	Bob Case	Black Hills Corporation	X		X	X	X	X				
55.	Individual	Trevor Tidwell	Texas-New Mexico Power Company (TNMP)	X									
56.	Individual	Richard Salgo	Sierra Pacific d/b/a NV Energy	X									
57.	Individual	E. Hahn	MWDSC	X						X			
58.	Individual	Fed Meyer	The Empire District Electric Company	X		X		X					
59.	Individual	Gary Ofner	North Carolina Electric Membership Corporation (NCEMCS)			X	X	X					
60.	Individual	Gordon Rawlings	British Columbia Transmission Corp. (BCTC)	X	X								
61.	Individual	James jones	Southwest Transmission Cooperative, Inc. (SWTC)	X									
62.	Individual	James Sharpe	South Carolina Electric and Gas (SCEG)	X		X		X	X				
63.	Individual	John Blazekovich	Exelon	X		X		X					
64.	Group	Denise Koehn	Bonneville Power Administration, Transmission Reliability Program (BPA Trans)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Curt Wilkins	BPA Transmission, System Operations	WECC	1
2.	Kelly Hazelton	BPA Transmission, System Operations	WECC	1
3.	Dick Winters	BPA Transmission, Substation Operations	WECC	1
4.	Kevin Dorning	BPA Transmission, PSC Technical Services	WECC	1
5.	Tom Gist	BPA Transmission, CC HW Dsgn/Stds Montr & Admin	WECC	1
6.	Sharon Brown	BPA Transmission, Project and Planning Support	WECC	1
7.	Mike Viles	BPA Transmission, Technical Operations	WECC	1
8.	Kevin Carman	BPA Transmission, Planning & Asset Management	WECC	1
9.	Rita Coppernoll	BPA Transmission, SPC Technical Svcs	WECC	1

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		10. Deanna Phillips	BPA, FERC Compliance Office	WECC	1, 3, 5, 6								
		11. John Wylder	BPA Transmission, CC HW Dsgn/Stds Montr & Admin	WECC	1								
		12. James Phillips	BPA Transmission, System Operations	WECC	1								
65.	Individual	Roger Champagne	Hydro-Québec TransÉnergie (HQT)	X									
66.	Individual	Chris Lyons	Constellation Energy Commodities Group (CCG)			X							
67.	Individual	Robert K. Loy	Allegheny Energy Supply Company, LLC (Allegheny Supply)					X					
68.	Group	Michael Gammon	Kansas City Power & Light (KCPL)	X		X		X	X				
		Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
		1. Jennifer Flandermeyer	KCPL	SPP	1, 3, 5, 6								
		2. Todd Fridley	KCPL	SPP	1, 3, 5, 6								
69.	Group	Kara Dundas	Conectiv Energy Supply, Inc.					X	X				
70.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X					
71.	Group	Terrence Simon	Constellation Energy (Constellation Power Generation, Inc.) (CPG)					X					
72.	Group	Terry L. Blackwell	South Carolina Public Service Authority (Santee Cooper)	X									
		Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
		1. S. T. Abrams	Santee Cooper	SERC	1								
		2. Glenn Stephens	Santee Cooper	SERC	1								
		3. Jim Peterson	Santee Cooper	SERC	1								
		4. Rene' Free	Santee Cooper	SERC	1								
		5. Vicky Budreau	Santee Cooper	SERC	1								
		6. Wayne Ahl	Santee Cooper	SERC	1								
73.	Individual	Larry Saxon	OGE Energy Corp	X		X		X					
74.	Individual	Darryl Curtis	Oncor Electric Delivery LLC	X									
75.	Group	Mark Heimbach	PPL Supply (PPL Generation & PPL EnergyPlus)					X	X				
		Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
		1. James Batug	PPL Generation	RFC	5								
		2. Annette Bannon	PPL Generation	NPCC	5								
		3. Mark Heimbach	PPL EnergyPlus	RFC	6								

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
76.	Group	Jared Shakespeare	City of St. George			X		X				X	
77.	Individual	Saurabh Saksena	National Grid (NGRID)	X		X							
78.	Individual	Joseph DePoorter	Madison Gas and Electric Company (MGE)			X	X	X	X				
79.	Group	Doug Hohlbaugh	FirstEnergy Corp. (FE)	X		X	X	X	X				
		Additional Member / **Additional Organization** / **Region** / **Segment Selection**											
		1. Rob Martinko / FirstEnergy / RFC / 1, 3, 4, 5, 6											
80.	Individual	Ron Donahey	Tampa Electric Company (TECO)	X		X		X	X				
81.	Individual	Ramona Marino	Snohomish County PUD				X						
82.	Individual	CJ Ingersoll	Constellation (CECD)										
83.	Group	Carol Gerou	Midwest Reliability Organization (MRO)										X
		Additional Member / **Additional Organization** / **Region** / **Segment Selection**											
		1. Tom Webb / WPS / MRO / 3, 4, 5, 6											
		2. Terry Bilke / Midwest ISO Inc. / MRO / 2											
		3. Jodi Jenson / Western Area Power Administration / MRO / 1, 6											
		4. Ken Goldsmith / Alliant Energy / MRO / 4											
		5. Dave Rudolph / Basin Electric Power Cooperative / MRO / 1, 3, 5, 6											
		6. Eric Ruskamp / Lincoln Electric System / MRO / 1, 3, 5, 6											
		7. Joseph Knight / Great River Energy / MRO / 1, 3, 5, 6											
		8. Joe DePoorter / Madison Gas & Electric / MRO / 3, 4, 5, 6											
		9. Scott Nickels / Rochester Public Utilties / MRO / 4											
		10. Terry Harbour / MidAmerican Energy Company / MRO / 1, 3, 5, 6											
84.	Individual	Anthony Wright	Georgia Transmission Corporation (GTC)	X									
85.	Individual	Jon Kapitz	Xcel Energy	X		X		X	X				
86.	Individual	Alan Gale	City of Tallahassee					x					
87.	Individual	Bill Keagle	GBE	X									
88.	Individual	John Allen	City Utilities of Springfield, Missouri	X									
89.	Group	Silvia Parada Mitchell	Florida Power & Light (FPL)	X		X		X	X				
90.	Group	William J. Gallagher	Transmission Access Policy Study Group (TAPS)										
91.	Individual	William J. Smith	Allegheny Power	X									
92.	Individual	Frank Gaffney	Florida Municipal Power Agency (FMPA)			X	X	X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
93.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
94.	Individual	Randy MacDonald	NBSO		X								
95.	Group	Edvard Lauman	Acumen Engineered Solutions International Inc. (AESI)										
96.	Individual	Dan Rochester	Independent Electricity System Operator (IESO)		X								
97.	Individual	Kasia Mihalchuk	Manitoba Hydro (Manitoba 2)	X		X		X	X				
98.	Individual	OMPA	Oklahoma Municipal Power Authority (OMPA)				X						
99.	Individual	Jason Shaver	American Transmission Company (ATC)	X									
100.	Individual	Eric Ruskamp	Lincoln Electric System (LES)	X		X		X	X				
101.	Individual	Catherine Koch	Puget Sound Energy (PSE)	X									
102.	Group	Scott Berry	Indiana Municipal Power Agency (IMPA)				X						

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Jenner	City of Edinburgh, Indiana	RFC	

103.	Individual	Christine Hasha	ERCOT ISO		X								X
104.	Group	Sandra Shaffer	PacifiCorp	X		X		X	X				
105.	Group	Ben Li	IRC Standards Review Committee and Security Working Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	James Castle	NYISO	NPCC	2
2.	Bill Phillips	MISO	MRO	2
3.	Mark Thompson	AESO	WECC	2
4.	Patrick Brown	PJM	RFC	2
5.	Matt Goldberg	ISO-NE	NPCC	2
6.	Steve Myers	ERCOT	ERCOT	2
7.	Lourdes Estrada-Salinero	CAISO	WECC	2
8.	Charles Yeung	SPP	SPP	2
9.	Dave Dunn	IESO	NPCC	2
10.	Tobias Hendricks	MISO	MRO	2
11.	Kelly Ryan	MISO	MRO	2
12.	Elliot Gordon	NYISO	NPCC	2
13.	Brett Lewis	NYISO	NPCC	2

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
		14. Gregory Goodrich	NYISO NPCC 2										
		15. John McGlynn	PJM RFC 2										
		16. Steve McElwee	ERCOT ERCOT 2										
		17. Jim Brenton	ERCOT ERCOT 2										
		18. Ann Delenela	ERCOT ERCOT 2										
		19. Garry Spicer	SPP SPP 2										
		20. Philip Propes	SPP SPP 2										
		21. Ryan McCon	SPP SPP 2										
		22. Tim Lockwood	CAISO WECC 2										
		23. Jamey Sample	TVA SERC 2										
		24. Joe Pereira	ISO-NE FRCC 2										
106.	Group	Richard Kafka	Pepco Holdings, Inc.	X		X		X	X				
		Additional Member	**Additional Organization** / **Region** / **Segment Selection**										
		1. Richard Kafka	Potomac Electric Power Company RFC 1										
		2. Mark Godfrey	Delmarva Power & Light RFC 1										
		3. Timothy Hadfield	Delmarva Power & Light RFC 1										
107.	Group?	Bill Gross	NEI										

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

Summary Consideration: A number of respondents' comments indicated some confusion between the definitions of Cyber System and BES Cyber System. Many also commented that the definition of Cyber System was too broad. The SDT considered these comments, has removed the definition of Cyber System since it is not referenced in the standard, and has modified the definition of BES Cyber System to include some of the concepts in the original definition of Cyber System into a single definition for BES Cyber System.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
Progress Energy	Disagree	Change to read: "A discrete set of one or more routable or dial-up programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data."
GSOC/OPC	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn't in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define "systems" as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word "organized" should be changed to "configured".
Hayden	Agree	1. Consider inclusion of "testing" in the list of functions. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? As I think through the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. Suggest you specifically address this and any other quesitons from FAQ for CIP-002 in the standard.
SDGE	Disagree	We feel that this is an overly broad definition for relevant cyber systems. We suggest rewording the Cyber System definition as follows: A discrete set of one or more programmable devices organized for the collection, storage, processing, maintenance, and communication of data". Under the proposed definition of Cyber System, certain non-relevant items could be in-scope that are unnecessary. We think it is more prudent to limit the scope and potentially eliminate unnecessary confusion.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
APPA	Agree	However, see below the discussion of BES Cyber Systems.
Consumers	Disagree	There is no need to introduce this term. See Section 13. This definition seems to include all electronic components within a substation, many of which either have no control capability or cannot independently control elements of the BES. eg, a simple electronic panel meter with no outside (the ESP) connectivity would be included. We'd suggest the following wording: "A discrete set of one or more programmable electronic devices capable of controlling elements of the BES and which is/are accessible remotely. We would go on to further define "access remotely" with the same criteria used in CIP-002-3, R3, of "… uses a routable protocol" or "is dial-up accessible". In addition, this definition, and other NERC guidance documents seem to imply that entire SCADA systems, Remote Relay Setting (or file acquisition) Systems, etc, would be included, even though only the portion located at the Control Center would be accessible via any commonly know threats utilizing dial-up or routable protocols. This change in terms would then include individual RTUs, relays, fault recorders, regardless of the fact these present an almost non-existent risk of being hacked. Although we respect the intent of trying to cover "systems" the definition cannot be so broad to thereby include every piece of every system, regardless of its unessential BES reliability contribution or the lack of accessibility to it remotely. NERC should refrain from using the word "risk". As a caller pointed out there is confusion as to whether impact or probability is the intended meaning. Specifically, in the definition of High BES Impact, take out the words "an unacceptable risk" after the word create in both instances it is used in the definition. "An unacceptable risk" also appears in the definition of Low BES Impact, it should be removed from there also.
NPCC	Agree	
SWPA	Disagree	With inclusion of BES Cyber System definition with proposed changes (below), this definition is not needed. This definition should be deleted and BES Cyber System definition changed as written in comment for 1.b.
MPPA	Agree	
Central Lincoln	Disagree	Since all cyber components are generally interconnected, it is unclear where one system ends and another begins. Any set chosen will have connections to other sets, and therefore not be a discrete set. Discrete: adj. Consisting of unconnected distinct parts.
Dominion	Disagree	Dominion proposes the definition be modified to state: "Cyber System — A discrete set of one or more Cyber Assets that communicate via routable protocol." As currently defined, the term would apply to all programmable electronic devices and expand the scope of applicability without providing additional reliability to the Bulk Electric System. The modified definition clarifies the intent of the term by limiting the scope of applicability to programmable electronic devices and communication networks (including hardware,

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		software, and data), all of which have the potential to adversely affect the Bulk Electric System.
Encari	Disagree	Requirement R3.1 implies that any Cyber System within a BES Subsystem that is identified under the criteria in Attachment 1 has the potential to be a BES Cyber System. That may not be the case since the definition of a Cyber System is not tied or related to the definition of a BES Subsystem. In order to ensure the implied relationship exists, we recommend the definition of BES Cyber System be expanded to state, "A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. A Cyber System associated with a BES Subsystem identified under the criteria in Attachment 1 is presumed to be a BES Cyber System if the Cyber System has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System."
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the proposed definition is overly broad and may include systems unrelated to the Bulk Electric System. Therefore, SCE proposes that the definition be more narrowly defined by adding the phrase "which support functions essential to the bulk electric system" to the end of the proposed definition.
USBR	Agree	
Dyonyx	Disagree	We believe there needs to be some clarification of the issue of "Communications equipment" being included or excluded as a BES Cyber System. Will an Entity that owns their "communication equipment (e.g., microwave system)" be required to classify and then apply security controls while an Entity that does not own its "communications equipment" (i.e., uses TELCO T1s, etc.) not be required to apply controls?
FMPP	Agree	
Westar	Agree	
Green Country	Agree	
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Wolverine	Agree	
Portland GE	Disagree	PGE does not agree with this definition for several reasons, including the fact that it does not specify something that "communicates," which is the risk these standards are attempting to address. Rather, it uses the even more ambiguous term "programmable;" this word must be defined. In addition, the word "critical" is being eliminated so that all systems are identified and ranked. That would imply that CIP is also an outdated term and may change to SIP or System

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Infrastructure Protection. The concept of ranking all grid facilities seems ambitious, and PGE questions whether the benefits of such a broadly scoped endeavor would justify the costs.
PSEG	Disagree	Comment #1: There are a number of new terms introduced. We would like a description of how the terms interrelate with each others and how the related to the previous version terms used such as “Cyber Asset” and “Critical Cyber Asset”. • More formalism is required to define what elements can constitute or be part of each term. For example, are Generation Subsystems a type of BES Subsystem or a constituent of a yet undetermined BES Subsystem? • Is a particular BES Cyber System to be treated as a single “atomic” entity or is a BES Cyber System composed of cyber assets that need to be investigated separately. • What is the definition of the word “element” used in the definitions of Generation Subsystem and Transmission Subsystem? Should the phase shared “shared Cyber System” be replaced with “shared BES Cyber System”? • The definition of what constitutes a Generation Subsystem or Transmission subsystem is whether these categorizations of assets “… become unavailable due to loss or compromise of a shared element of a shared cyber system”. How can this italicized statement be known a prior? Categorization is BES Subsystem is an R1 requirement that is not dependent on knowledge of whether a “cyber asset” can be compromised. Comment #2: What does the group mean by a programmable electronic device for “maintenance”, “communication” and “use”? (Could the SDT please provide an example of each type of device?) Comment #3: Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? Comment #4: We believe that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be program over the internet or through a routable device.) EEI’s proposed definition for Cyber Systems: “Cyber System – a discrete set of one or more programmable electronic devices organized in a collection , storage ,processing , maintenance , use , sharing, communication, disposition or display of data WHICH SUPPORTS FUNCTIONS ESSENTIAL TO THE BES ..” seems to better define the term. Comment #5: We believe that the monitor’s which only display data should not be included as part of a Cyber System. Our understanding: We understand the term, “Cyber System” to imply one or more electronic device(s) that are part of an interconnected (networked) within an Electronic Security Perimeter (ESP) with the capability to be programmed remotely (offsite). Comment #6: We are concerned about the inclusion of maintenance, sharing, communication, disposition, and display. Comment #7: There is no need to introduce this term. Suggestion:

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		"Has the capability to remotely acquire and modify real-time BES system data, send control signals to, or modify the settings of a programmable electronic device(s)." Our suggestion addresses either "open" (e.g. internet), "closed" (e.g. private fiber optic network) or a combination of the two different network configurations. Entities must be allowed the ability to factor in their network configuration as part of the engineering analysis
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. The current definition is too broad and implies the inclusion of electronic devices that would not have anything to do with the BES. The definition of Cyber System does not include the category of control. We further recommend more clarity in the list of attributes. For example, does "maintenance" apply to test equipment, data, etc.? A cyber system has traditionally been identified as one that uses a routable protocol and therefore can be network connected.
Idaho Power	Disagree	Programmable electronic devices could be interpreted to exclude certain types of cyber assets. Replace with cyber assets instead.
SOCO	Disagree	This definition will force inclusion of all electronic components within a substation, many of which either have no control capability or cannot independently control elements of the BES. Suggest the following wording: "A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data and has the ability to independently control elements of the BES." The term as defined would include most if not all instrumentation equipment installed within a Generation Unit. Even a simple stand alone 4-20 mA control loop consisting of a typical pressure transmitter, control panel mounted analog controller and a control valve, with no connection possibility to any "network", would be included in the defined scope of a "Cyber System". Within the described loop any of three components would trigger inclusion. All of these devices are programmable from the standpoint that their calibration parameters may be adjusted and the related setting stored to local onboard memory. Care should also be taken in the wording to avoid inclusion of terms, which could include technology such as HART protocol, which allows configuration based on physical access to the device or connection to the analog signal control wiring at the same geographic location. As presently written this definition would include even temporary performance monitoring and testing systems which are used for data acquisition and performance enhancement and which in no way connect to control and command systems or have a potential to impact the operation of a generation unit. This definition should address only those upper level systems, which are capable of being electronically accessed and manipulated from an offsite location. Suggested definitions are: Cyber System – A set of one or more "remotely accessible" programmable electronic devices organized for the collection, storage processing maintenance use sharing, communication, disposition or display of data.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
DTE	Disagree	This definition needs revision to remove devices that do not use routable protocols from the scope of the standard. Similarly communication networks between discrete ESPs should not be in scope.
AEP	Disagree	AEP appreciates the extensive efforts of the SDT in the preparation of the version 4 draft standard. The SDT may well be trying to provide registered entities with greater flexibility in defining its applicable assets and systems, but the open-ended nature of this definition and of the standard in general, is of concern. Ultimately, the audit teams will determine if the registered entity included the assets and systems that it should it should have and, to this end, most entities would prefer to have “bright lines” that clearly state what is in scope and out of scope. Without some limitations, all programmable devices may be considered cyber assets, including those not connected to a network could be included as in scope under the provided definition. For example, all generator and transformer digital protective relays could be considered in scope even if its not network connected. Risk levels will differ based on the type of interface, connection, and controls. The standard language is even blurring the line between computers and control system equipment. Alternatively, we would suggest adopting the Control System definition from NIST SP800-82 and striking the Cyber System definition. NIST SP800-82 makes it abundantly clear that industrial control systems are different than traditional IT systems. Consistent with FERC’s Order, it would be helpful to the team to leverage this NIST work as it highlights the work industries and government organizations are to advance control system security. Accordingly, the suggested Control System definition would be: An information system used to control processes such as manufacturing, product handling, production, and distribution. These systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Disagree	N&ST believes, based on experience with the current Standards, that definitions intended to allow for flexibility and to "cast a wide net" tend to lead to endless, and often unproductive, debate over their precise meaning. At a minimum, we recommend that the SDT consider addressing both the logical and *physical* proximity of a "cyber system's" components in order to forestall arguments over whether or not a "cyber system" can span multiple locations (e.g., a set of field assets, such as RTUs, feeding data to a control center at another location).
Flathead	Disagree	I do not think constantly creating new definitions without clarifying existing definitions and acronyms is efficient. I believe the existing definitions should be retained or modified. Also the Bulk Electric System vs. the Bulk Power System, the most key definition of all is still not properly clarified by the regions. Shouldn't that be the focus before creating new subsystems that may include both BES and non-BES assets. This definition has the potential of diverting resources to non-critical non-BES assets that are truly "low impact" and should not be part of this evaluation, defeating the purpose of protecting critical assets.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
E ON	Disagree	The definition would include standalone devices, i.e., non-networked devices, that perform any one of the listed functions. Keeping in mind the purpose of preventing unauthorized access, the definition is far too inclusive. A stand-alone programmable logic controller cannot be accessed except by an individual in the plant with proper MMI. An on premises individual could disable plant operations far more easily by simply operating switches on the control panel.
Carthage	Agree	
WECC	Agree	The word programmable might lead to confusion in the future as entities may be unsure if it refers to programmable by them or the manufacture or both. The word doesn't seem necessary in the definition.
Entergy	Disagree	Anything with EPROM would seem to apply, though may not necessarily be relevant.
CenterPoint	Disagree	CenterPoint Energy does not support the direction the SDT is taking with the introduction of multiple new definitions. One of the four key principles driving the SDT's work is to "build on work already done to comply with Version 1 of the CIP reliability standards, including the industry's experience and investments." The proposed changes do not align with that principle and in fact appear to start over with new concepts. Considering the considerable effort that registered entities have already expended to comply with the existing standards under the existing categorization of assets, it does not make sense to "reinvent the wheel" at this juncture. Furthermore, the proposed new set of definitions in CIP-002 would be incompatible with CIP-003 through CIP-009. CenterPoint Energy understands the SDT's intent would be to conform CIP-003 through CIP-009 over time in some piecemeal fashion to the new paradigm introduced in this version of CIP-002. CenterPoint Energy believes the SDT's piecemeal implementation plan is unrealistic and will add even further confusion to the CIP standards. Indeed, much of the CIP-003 through CIP-009 requirements would not make sense for anything other than Critical Assets, roughly equivalent to the proposed "High BES Impact" paradigm introduced in this draft. A specific concern with the proposed definition of cyber system is the inclusion of "communication" as one of the possible attributes that define a cyber system. The considerable vetting by the industry over the many years produced the appropriate conclusion that communication devices are outside the definition of BES cyber assets. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are exempt from the existing Standard CIP-002 in section 4.2.2. This exemption should remain in version 4 because these common carrier communication lines are often leased from third party telecommunication companies who should be responsible for the protection. CenterPoint Energy believes the SDT may have intended to capture the concept from the existing CIP-002 version that an electronic device must communicate by routable or dial-up communication mediums in order for the device to be considered a cyber asset. However, as written, one could misinterpret the definition as meaning that communication mediums themselves are cyber assets, which would not be appropriate. The definition of a cyber system should be reworded as follows: Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, which communicates externally

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		through a routable or dial-up communication protocol.
CA Cogen	Agree	
LCRA	Agree	
FRCC	Disagree	The Definitions proposed by the SDT for Bulk Electric System Subsystem states, "A group of one or more BES Facilities…". Per the NERC Glossary of Terms a Facility is a set of electrical equipment that operates as a single BES Element. Therefore a subsystem is a group of elements and if you replace 'subsystem' with 'element' in the requirements the intent of the requirement remains intact and you are not introducing confusion by redefining a portion of the BES (i.e. BES Subsystem, Transmission Subsystem and Generation Subsystem). If additional clarity is desired by the SDT, a revision to the current definitions of Element, Facility and Transmission should be considered before new terms are introduced to the industry.
NIPSCO	Disagree	We are concerned about the inclusion of the terms maintenance, sharing, communication, disposition, and display. Suggestion: Further clarifications on the intent of this language as well as examples of device types are needed.
ConEd	Disagree	Real-time Operations: There should be a requirement that the system is used for real-time operation and/or to make real-time decisions. Interconnectedness: There should also be a requirement that the Cyber System is networked or connected somehow outside the station. The definition should include that the fiber system has connectivity to the outside environment such that it can be hacked. Cyber system assets are too broadly defined and the definition does not taking into account that the systems in many cases are protected by physical isolation, locked cabinets and/or rooms.
EEI	Disagree	EEI believes that this definition is overbroad and potentially brings in an inappropriate number of devices that should not be in scope for the standard, e.g. display terminals, personal cell phones, pagers etc. The definition of Cyber System includes "communication." This phrase should either be defined more precisely or removed. The definition of Cyber System includes "disposition." This phrase should either be defined more precisely or removed. EEI suggests the following revision: Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access, that support functions essential to the bulk electric system.
O&R	Disagree	Real-time Operations:

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		There should be a requirement that the system is used for real-time operation and/or to make real-time decisions. Interconnectedness: There should also be a requirement that the Cyber System is networked or connected somehow outside the station. The definition should include that the fiber system has connectivity to the outside environment such that it can be hacked. Cyber system assets are too broadly defined and the definition does not taking into account that the systems in many cases are protected by physical isolation, locked cabinets and/or rooms.
Alliant	Agree	
Ameren	Disagree	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. Also, if “communication” devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of Cyber System includes “disposition.” This phrase should either be defined more precisely or removed. Add to the end of this definition “that together perform a specified function”.
Black Hills	Agree	The definition itself is technically sound, but it implication is profound because virtually all programmable electronic devices would be included by the definition.
TNMP	Disagree	TNMP believes the current Cyber System definition fails to establish clear criteria or “bright lines” the drafting team is attempting to put into the standards. The definition fails to clearly convey how the discrete sets of devices are grouped together into a Cyber System. Some statement binding the devices based upon function or mission objective would help. However, the reason for a revision of CIP-002 is to eliminate the Responsible Entity from being tasked with developing a risk methodology and to create a uniform methodology across the industry. The proposed standard shifts the problem of defining Critical Cyber Assets to defining Cyber Systems without appreciably addressing industry uniformity. The definition needs to be greatly improved since it is the basis definition for BES Cyber System to which future CIP-003 through CIP-009 standards apply. A few examples of how the current definition lacks clarity: Is a SCADA System restricted to Master servers and operation workstations? Are the RTUs which reside in many BES Subsystems included in the proposed definition? Does RTU communication system architecture (e.g. centralized modem bank, distributed banks with Ethernet conversion, direct Ethernet) contribute to determination if the RTUs are Cyber Systems? Are RTUs and their communication systems to be considered part of the SCADA Cyber System? Can isolation of communication systems via network firewalls exclude devices such as RTUs from inclusion in a SCADA

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		system? Should the RTUs be considered part of the SCADA Cyber System given that the ability to manipulate the RTU in a manner that would result in successful manipulation of the main SCADA Cyber System is extremely limited and unlikely? Other examples of lack of clarity arise in the application of the definition to the relay systems in a substation: Would a Relaying Cyber System be comprised only of devices within a single substation or all relaying across any connected substations? Would the Relaying Cyber System be grouped by the relays interaction with other relaying? This possibility could result in several relay systems along a transmission path being considered a singular Relay Cyber System. In summary TNMP believes the current definition lacks clarity to help the industry implement meaningful cyber security measures, and makes it difficult for NERC to properly audit Responsible Entities uniformly.
NVEnergy	Disagree	The use of the qualifier “one or more” leaves open the question of what discretion is allowed the Entity to group these devices together. We believe this will lead to confusion or inconsistency in application. We suggest to the Standards Drafting Team that this definition be restricted to the discrete cyber device level, rather than allowing discretion as to the number of cyber devices that should be collected to form a “system” Also, the very word “Cyber” should require that the system is accessible via remote locations from the device.
MWDSC	Disagree	Too vague a definition which could apply to any electronic device within a local facility. Needs to include some form of communication device, e.g., RTU or modem, which interfaces with a control center. For example, some protection devices in substations automatically react to power flows and do not require a control signal from a remote location. Recommend adding a phrase at the end such as "..,or display of data, and communicated to a Control Center at a remote location."
Empire	Disagree	Option for consideration for definition of Cyber System: Programmable electronic devices and communication networks including hardware software and data.
NCEMCS	Disagree	I Agree in concept, however this definition includes all electronic devices of which many will have no control capability or cannot independently control elements of the BES
BCTC	Disagree	See Question 13
SWTC	Disagree	SWTC has some concerns with this new standard, as it all based on BES Assets, and their impact. I am under the assumption that the Bulk Electric System Task Force is trying to rewrite the BES Definition. It appears that until the BES is defined, then any assumptions presented in CIP-002-4 are under the old definition, which is almost like putting the cart before the horse.
SCEG	Disagree	While the majority of cyber systems may be organized for the data purposes described, others only use data as a tool for another purpose. For instance, a physical access control cyber system is not organized for the collection, etc. of data. The data is simply a means to an end. It is organized for access control. The definition could be improved by avoiding the

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		concept of what the system is for entirely. Suggested wording: "A discrete set of one or more programmable electronic devices that collects, stores, processes, maintains, uses, shares, communicates, disposes of, or displays data." We also feel that "Test and Validation" and "Recovery" should be added to the definition.
Exelon	Disagree	Exelon has concerns with the proposed CIP standard definitions that may result in overlaps and/or conflicts in definitions between the regulatory entities (NRC, CNSC, and NERC). We ask that NERC and/or the SDT take action to ensure the proposed definitions are reviewed and revised if needed to eliminate any potential overlaps. Exelon also has concerns with the ambiguity introduced into the definition by including “communication” and “disposition”. We suggest the following as the definition: Cyber System – A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing or display of data which support functions critical to the Reliable Operation of the Bulk Electric System (i.e. Attachment 2)
BPA Trans	Disagree	This definition is better than the one for Cyber Assets but still leaves some unanswered questions regarding exactly what would qualify as a Cyber System. The term “programmable electronic device” must be defined. The following definition is suggested: "capable of executing code installed into volatile memory by end users". If not defined, then the use of the word “programmable” is problematic. Many industrial control devices, which may use microprocessors, can have their settings changed and could be considered “configurable,” but users cannot “program” them in the classic IT sense of the term. The base functions of onboard software cannot be changed nor can new software be written, compiled, or installed on them except by the vendor. Question 1: Is it intended that the terms “set,” “configure,” or “program” are meant to be interchangeable with “programmable?” Question 2: Is a device that has a limited specific set of factory defined capabilities considered “programmable?” Some examples of installed equipment that need a determination of “programmable” are: • A device that is limited to being “set” or “configured” through a vendor provided user interface, within device limitations, or • A device not capable of having its base programming altered while in operation, or • A device that requires specific vendor supplied hardware to change or update, or • A device that must be flashed or have EPROMs replaced for updates, using vendor provided interface/ports and with vendor provided updates, or • A device not capable of having additional applications installed, or • A device that has no onboard memory locations that can hold extraneous programs.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Question 3: What about non-cyber "Cyber Systems," such as: • Devices that operate on a microprocessor platform and could be defined as Cyber Systems even though they have no other attributes of a Cyber System? These devices, while possibly providing support to the BES Subsystem, present no potential for vulnerability or degradation of the BES, or • Devices that only provide interface for viewing information, but cannot be controlled, nor does it provide control, or • Devices that are microprocessor based but have no communications connections, or • Devices that are microprocessor based which may be directly affected only physically at the device. • If the connection between two devices is a simple electrical on/off connection (firing of alarm points) does it constitute a Cyber System? • Is a microprocessor based relay (supports the operation of a BES Subsystem) but is not connected to any form of communications so must be assessed manually and operates autonomously, a "Cyber System?" The new definition of "Cyber System" is all-inclusive. It appears that the SDT intends to capture any and all electronic devices under the umbrella of this definition: Table of Purpose Elements and potentially included Devices/Systems: Purpose Element Devices/Systems that may be included Collection (of data*) Relays, DFRs, SER, TTrip, PMU, RAS RTU, Controller and IDP Laptops, Others? Storage (of data*) Relays, DFRs, SER, TTrip, PMU, RAS RTU, Others? Processing (of data*) Relays, TTrip Controller and IDP Laptops, Others? Maintenance(of data*) Not sure how to address this one. Devices don't generally maintain data, people do. Use (of data*) Relays, Firewalls, Laptops, Others? Sharing (of data*) Interfaces on Firewalls, Relays, D400s, Others? Communication (of data*) Networks and other communications infrastructures? This is significant as it may draw in The FIN, SONET, DATS, Microwave Radio System, Modem Connections and other communications equipment. Disposition (of data*), or This may be the archiving or destruction of data. We are not sure. display (of data*) Web interfaces, Laptops, simple HMI interfaces, SEMM, RAS, Alarm Systems. What would be included?

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		* - The focus is on “data,” which is typical for security of IT systems. The argument can be easily made that nearly all electronic devices perform one or more of these functions. Is this what the SDT intended? The rest of the definition is almost straight out of the National Institute of Technology (NIST) Interagency Report 7298 (NISTIR-7298). We believe that this is good.
HQT	Agree	
Allegheny Supply	Agree	
KCPL	Disagree	No, this is too broad in regards to “of data”. The CIP Standards should limit themselves to the equipment and data used only for the monitoring and control of the BES.
Connectiv Energy	Agree	
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13. This definition is not needed at this time. If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time. Further, there is value in retaining the existing definitions of Critical Cyber Asset and Cyber Asset (but clarifying what is meant by “network”) and the qualifying characteristics of routable protocol or dial-up. Security controls will still be applied to distinct, discreet, individual Cyber Assets, not generically defined “systems.” If categorization proves the value and need for defining the term Cyber System, the definition should be “a group of Cyber Assets that communicate by routable protocol and/or are dial-up accessible.” This solves the problem with the draft definition in CIP-002-4 of being overly broad and bringing in a number of devices that should not be in scope because they are not vulnerable to a concerted, well-planned attack against multiple points; including, for example: display terminals, cell phones, pagers, as well as many kinds of devices that cannot be accessed or manipulated from a remote location.
CPG	Disagree	This definition of cyber system is extremely broad and encompasses too many items. What is lost in this definition is that these systems may not be critical to the operation or protection of the BES element, and would therefore not be critical to the BES. To have entities list every cyber system does not have an impact on the safety and reliability of the BES. This term should be combined into the BES Cyber System terminology.
Santee Cooper	Agree	Santee Cooper Introductory Comments: As a whole, Santee Cooper (SC) supports the general framework of the new version. However with this new version comes an enormous amount of procedural and policy overhauls. SC would support a phased-in approach as opposed to a deadline for compliance. In addition SC would not want to vote on this standard alone. Because new versions of CIP-003 through CIP-009 would also be required, and those would define the different levels of requirements for the impact levels, SC would rather vote on CIP—02 through CIP-009 as a total package.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
OGE	Disagree	• Provide a description for the term "disposition". What is your intent for including this term. • Provide a definition/description for the term "Communication" How does section "4. Applicability: 4.2.2. "Cyber assets associated with communication networks …." found in Standards CIP 002-1, CIP 002-2 and CIP 002-3. There is an exemption for cyber assets associated with communications between ESPs. Will this exemption carry to the version 4 standard? • Is there any processor based device that does not fit this definition?
Oncor	Disagree	There is no clarity as to what makes up a “cyber system”. Is my SCADA system a Cyber System? Is a single programmable relay at a substation a cyber system or do all the relays at a substation makeup a single cyber system?
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Disagree	1. Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? National Grid believes that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be programmed over the internet or through a routable device.) 2. Please provide example of programmable electronic device organized for “maintenance”, “use”, and “communication” 3. Monitors which only display data should not be part of Cyber System
MGE	Disagree	MGE understands why the SDT is defining Cyber System, establishing a basis for “BES Cyber System” but the proposed definition must clarify that it applies to Cyber Systems that support the reliable operation of the BES where as to maintain equipment and electric system’s thermo, voltage and stability limits so that instability, uncontrolled separation, or cascading failures do not occur, as written in question 1.g. As written, every computer, cell phone, or storage device (ie, thumb drive) would be considered a Cyber System no matter if it is for BES operations or personal use. Please clarify what “maintenance, communication and use” means in the proposed definition. The displaying of data (a monitor) should not be included. The displaying of data is received from a CPU or SCADA system, the monitor has no impact or ability to perform an action that would disrupt the BES. Recommend that the definition apply to devices that are electronically accessible. An electromechanical relay can be programmed but not via the internet or through a routable device.
FE	Disagree	The definition should be limited to programmable electronic devices that have the ability to be accessed remotely and pose risks to a coordinated attack. The definition is open-ended and could easily be misinterpreted and inadvertently include devices that would pose no risk to the BES; cell phones, pagers, computer terminals, etc.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		FirstEnergy offers a slightly modified version of the definition offered by EEI. We have removed the phrase "that support functions essential to the bulk electric system" from the EEI version as the BES Cyber System definition brings in that aspect. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access.
TECO	Disagree	Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data that supports functions essential to the bulk electric system.
CECD	Disagree	CECD supports having a separate definition for Cyber System. The definition should explicitly exclude analog devices and the communication networks and data communication links between discrete Cyber Systems. In addition, as indicated in our discussion on the definition of BES Subsystems, we do not feel it is appropriate to include a control center in that definition, but instead would prefer that the control center be defined as a Cyber System to be evaluated for its impact on/interaction with BES Subsystems to determine if the control center qualifies as a BES Cyber System.
MRO	Agree	The MRO NSRS approached every question as if it were in a vacuum, attempting to answer the individual questions honestly without being persuaded by the remainder of the standard. This meant addressing the questions as written and including comments only in the appropriate areas. While we may agree with the individual questions being asked, we request that the SDT give particular consideration to our comments found in question 13, which details our thoughts on the overall approach of the CIP-002-4 draft standard.
GTC	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn't in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define "systems" as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word "organized" should be changed to "configured".
Xcel	Agree	
BGE	Disagree	We believe that the definition of "Cyber System" is unnecessary and that item 1.a. should be deleted. The standard should only deal with BES Cyber Systems and this definition of Cyber System can be rolled into BES Cyber Systems.
Springfield, MO	Agree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		TAPS supports the comments submitted by the MRO NSRS regarding this project, as well as the modifications to the standard proposed by APPA. TAPS submits these separate comments to object to the proposed three-tier approach, and urge the inclusion of a fourth, "No Impact" tier. Specifically, TAPS emphasizes its concerns with respect to the treatment

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		of "Low BES Impact" subsystems and cyber systems, set out in response to Questions 1(i), 2, and 8, below. As this proposed standard appears to be largely implementing the Categorizing Cyber Systems Concept Paper issued by NERC in July 2009, please see as well TAPS' comments on the Concept Paper, submitted September 4, 2009.
Allegheny power	Disagree	AP believes that this definition is overbroad and potentially brings in an inappropriate number of devices that should not be in scope for the standard, e.g. display terminals, personal cell phones, pagers etc. The definition of Cyber System includes "communication." This phrase should either be defined more precisely or removed. The definition of Cyber System includes "disposition." This phrase should either be defined more precisely or removed.
FMPA	Disagree	Intro: First, let FMPA congratulate the CIP Standard Drafting Team for creating a good framework for identifying the focus of what is to be regulated concerning cyber security and focusing that regulation on what is important to ensuring BES reliability. Although FMPA has checked the "disagree" box on many of these questions, we believe the general framework to be sound and most of FMPA's comments are geared towards reducing the complexity of the standard, to help clear up ambiguity and reduce subjectivity, to contribute to the technical expertise discussions, and to increase the clarity of the standard. With those foci in mind, we offer the following comments which we hope you find constructive. Comments: One would assume that a Supervisory Control and Data Acquisition (SCADA) would be a Cyber System, yet there is no mention of "Control", which would seem to be the characteristic of a Cyber System with the highest impact to BES reliability.
Duke	Disagree	This definition should be revised to exclude field wired devices that happen to be programmable. Suggested wording: Cyber System – A discrete set of programmable electronic devices connected together via an active communications protocol.
AESI	Disagree	The term Cyber System appears to have replaced Cyber Asset in order to allow for greater flexibility in applying the remaining CIP standards, however as currently defined it also creates greater ambiguity regarding what is and isn't in scope. The definition of Cyber System is vague and needs additional clarification. For example, is our telecommunications network one Cyber System or are the communication devices at one physical location a Cyber System or is each piece of communication equipment a Cyber System? We suggest further clarifying the definition to define "systems" as only devices with a single function and within a single ESP. The definition should be modified to include control functions and limited to include only devices that are remotely accessible. The word "organized" should be changed to "configured".
IESO	Agree	
Manitoba 2	Disagree	Please clarify the meaning of the word "maintenance" as it applies in this definition. Please clarify the meaning of the word "disposition" as it applies in this definition. If the intent is to mean "the way in which something is arranged", that is included under display of data. If the intent is to mean "the transfer of property to

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		someone", that is included under sharing of data. The Cyber System definition needs to be clearer regarding the determination of the boundaries of a cyber system. Please define "programmable". Is every electronic device which is configurable by any means (switches, dials, settings) considered a "programmable" device? Should an electronic device, such as a protocol converter which is settable, be considered a cyber system, or is it really meant to focus on intelligent electronic devices and systems? Security requirements also need to consider the capabilities of the devices. Are cyber systems which primarily support a maintenance activity related to a BES Subsystem to be included in the scope of this definition? If, so how is it limited to the most important activities? Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Agree	
ATC	Disagree	Concerns with the proposed definition: 1. What does the group mean by a programmable electronic device for "maintenance", "communication" and "use"? (Could the SDT please provide an example of each type of device?) 2. Does this definition mean that the electronic device has to have the capability to be programmable (through an electronic means i.e. routable program or internet access) in order to qualify as part of a Cyber System? 2.1. ATC believes that this definition needs to clearly identify that this is limited to devices that are electronically accessible. (An electromechanical relay can be programmed but can not be programmed over the internet or through a routable device.) 3. ATC believes that the monitor's which only display data should not be included as part of a Cyber System. Our understanding: We understand the term, "Cyber System" to imply one or more electronic device(s) that are part of an interconnected (networked) within an Electronic Security Perimeter (ESP) with the capability to be programmed remotely (offsite). Suggestion: "Acquires / collects real-time BES system data, sends control signals to BES Facilities either through command functions or settings and is programmable by remote access." Our proposed definition is attempting to identify only those electronic devices that control an action or collect real-time data on the BES. We believe that this standard should not identify such devices as firewalls, switches or routers. This separation provides the SDT the ability to develop different controls around the distinct groups of devices and should result in the elimination of a number of current TFE requests. In addition, our suggestion addresses either "open" (e.g. internet), "closed" (e.g. private fiber optic network) or a

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.a. Comment (Response page 5)</th></tr>
<tr><td></td><td></td><td>combination of the two different network configurations. Entities must be allowed the ability to factor in their network configuration as part of the engineering analysis.</td></tr>
<tr><td>LES</td><td>Disagree</td><td>
We support the MRO NSRS comments with the following additional items:

If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate
</td></tr>
</table>

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).
PSE	Disagree	Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access. Puget Sound Energy supports the inclusion of all definitions in the NERC Glossary with used consistently across all standards versus localized definitions that differ across different applications.
IMPA	Disagree	IMPA proposes the following definition for Cyber System. Cyber System - A discrete set of one or more programmable electronic devices grouped together to perform the following functions: the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data as required by Control Centers, Generation Subsystems, and/or Transmission Subsystems for the reliable operation of the Bulk Electric System.
ERCOT	Disagree	The current definition lends itself to misinterpretation and expansion of the intent. Recommend that the definition clarify that a Cyber System as a discrete system where all components contained within act as common functional elements of the system and individual components, whether or not they are capable of being programmed, are not considered separate Cyber Systems. Request that the drafting team provide clarification regarding categorization and classification of cross platform infrastructure systems. This should include guidance on components that are exchangeable or hot swappable without any impact on the Cyber Systems utilizing that component.
PacifiCorp	Disagree	See PacifiCorp's summary comments in question 13. This definition is not needed at this time. If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time. Further, there is value in retaining the existing definitions of Critical Cyber Asset and Cyber Asset (but clarifying what is meant by "network") and the qualifying characteristics of routable protocol or dial-up. Security controls will still be applied to distinct, discreet, individual Cyber Assets, not generically defined "systems." If categorization proves the value and need for defining the term Cyber System, the definition should be "a group of Cyber Assets that communicate by routable protocol and/or are dial-up accessible." This solves the problem with the draft definition in CIP-002-4 of being overly broad and bringing in a number of devices that should not be in scope because they are not vulnerable to a concerted, well-planned attack against multiple points; including, for example: display terminals, cell phones, pagers, as well as many kinds of devices which cannot be

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		accessed or manipulated from a remote location. .
PEPCO	Disagree	Parts of the Cyber System definition are too broad and overreaching with the potential of including unintended devices that do not necessarily need to be in-scope. Not all programmable devices are able to be reprogrammed or have the storage capacity to have an Operating System. The definition as presently written could include coffee makers, televisions, radios, mp3 players, DVDs, PC projectors, telephones, watches/clocks, USB storage devices, thermostats, thermometers, navigation systems, pagers, barcode scanner, and/or 2-way radios. The definition seems to focus on data (e.g. storage, maintenance, use, sharing, displaying) and not necessarily on cyber control systems which should be the main focus. The current definition could lead to confusion. Clarity and more precise definitions are needed for terms such as – a discrete set of one, programmable electronic devices, communication, and disposition of data. . We suggest the following: Cyber System - Suggest that the define term of Cyber System not be used. Rather start off with the BES Cyber System definition. If the SDT feels that this term is still needed, suggest that examples of “Cyber System” devices be provided for each item included in the definition (e.g. collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data) to provide clarification.
NEI	Disagree	A) It does not describe the functions, and the use of “data” is vague and needs better definition. B) There is no language about routable protocols – need to add “that communicate via a routable protocol.” C) NEI recommends “A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, or display of data which can be operated or controlled by remote access.” D) The SDT may well be trying to provide registered entities with greater flexibility in defining its applicable assets and systems, but the open-ended nature of this definition and of the standard in general, is of concern. Ultimately, the audit teams will determine if the registered entity included the assets and systems that it should have and, to this end, most entities would prefer to have “bright lines” that clearly state what is in scope and out of scope. Without some limitations, all programmable devices may be considered cyber assets, including those not connected to a network could be included as in scope under the provided definition. For example, all generator and transformer digital protective relays could be considered in scope even if it is not network connected. Risk levels will differ based on the type of interface, connection, and controls. The standard language is even blurring the line between computers and control system equipment. E) Alternatively, we would suggest adopting the Control System definition from NIST SP800-82 and striking the Cyber System definition. NIST SP800-82 makes it abundantly clear that industrial control systems are different than traditional IT systems. Consistent with FERC’s Order, it would be helpful to the team to leverage this NIST work as it highlights the work industries and government organizations are doing to advance control system security.

Organization	Yes or No	Question 1.a. Comment (Response page 5)
		Accordingly, the suggested Control System definition would be: An information system used to control processes such as manufacturing, product handling, production, and distribution. These systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Summary Consideration: A number of respondents' comments indicated some confusion between the definitions of Cyber System and BES Cyber System. Many also commented that the definition of Cyber System was too broad. The SDT considered these comments, has removed the definition of Cyber System since it is not referenced in the standard, and has modified the definition of BES Cyber System to include some of the concepts in the original definition of Cyber System into a single definition for BES Cyber System.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
Progress Energy	Disagree	Add the following to the end of the definition: "as defined in CIP-002-4 Attachment 1."
Dynegy	Disagree	Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems "also includes all of the components necessary to ensure the protection of the reliability function(s) being performed". If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
GSOC/OPC	Disagree	If "functions critical to the reliable operation of the Bulk Electric System" is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2. The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
Hayden	Agree	
SDGE	Disagree	"Critical" and "adversely" need to be defined or have examples provided. Even the phrase "has the potential" lends additional vagueness to the definition. We are advocating a simpler approach to make the definition easier to understand and apply. We propose the following wording: A Cyber System, which if rendered unavailable, degraded, or compromised, would impact the reliable operation of the BES.
APPA	Disagree	APPA Task Force Prefatory Comments: The APPA CIP Task Force supports the general framework for BES cyber-security proposed by the CS706 Standards Drafting Team ("the SDT") and commends the team for its work. While we have checked "Disagree" for many of comment boxes below, in each case we have attempted to provide constructive comments to improve upon the clarity and quality of the draft standard and where possible, to simplify the steps that registered entities must undertake to

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		ensure both BES cyber-security and auditable compliance. Should you have any questions concerning these comments, please do not hesitate to contact us. We look forward to reviewing and commenting upon the next draft of CIP-002-4, as well as the associated security controls being developed under CIP-003-4 through CIP009-4. APPA Task Force Suggested Definition: BES Cyber System - A discrete set of one or more programmable electronic devices that are organized to control generation or transmission and/or gather data, essential for the real time operation of the BES, which if rendered unavailable, degraded or compromised, has the potential for an Adverse Reliability Impact. This definition will limit the scope to address vulnerabilities related to a cyber attack on systems that impact the real time operation of the BES. If it is the intention of the drafting team to include systems that do not directly affect real time operations, then it is our recommendation that this should be addressed in another standard(s). The NERC Glossary of Terms should be used when there are defined terms available for use. Adverse Reliability Impact is such a term.
Consumers	Disagree	This needs to be specific to at risk cyber systems. There are cyber systems that could adversely impact the reliability of the BES that are not at risk since they do not use routable protocols. The definition of critical cyber assets was more descriptive and better suited the intent of the reliability standards. This seems to simply be another way of saying the system or device is a Critical Cyber Asset (CCA) and provides no further benefit. In addition, the phrase: “has the potential to adversely impact” is too vague. For example, a device such as a controller, RTU, relay could be unavailable for an extended period of time and have an ‘adverse impact’ in that it is certainly inconvenient. However, since protection and control system operations on the BES are automatic and independent of SCADA control, loss of an RTU, for whatever reason, is not immediately or by default a critical situation. In addition, there needs to be recognition that if the devices are not networked, and access to one device cannot easily lead to other devices, the concern is minimal and therefore not critical (or a BEC Cyber System, by this definition) There appears to be a conflict of the definition with the category of a “Low” BES Subsystem as a low classification (and thus its related cyber system) cannot adversely impact the reliable operation of the BES. We are struggling to see how a classification of “Low” could possibly have a BES Cyber System which is critical to the reliable operation of the BES, so it would appear that there would never be BES Cyber Systems for Low Subsystems! Suggested definition: A Cyber System which if remotely accessed (via a routable protocol or dial-up) and rendered unavailable, degraded, or compromised has the potential to initiate, disable or compromise (through direct command or setting changes) operating functions critical to the reliable operation of the Bulk Electric System or essential for the operation of a generation unit which could adversely impact the reliable operation of the BES.
NPCC	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” The definition is not clear, creates audit issues. Needs to be more explicit on what the definition of boundaries of cyber system applicability are. (Attachment 2 to be considered).

Organization	Yes or No	Question 1.b. Comment (Response page 6)
SWPA	Disagree	A definition should focus on the meaning of the phrase, not place parameters around it such as “which if”. A more concise definition would be “A discrete set of one or more programmable electronic devices organized to control and/or monitor the real-time operation of the BES.”
MPPA	Agree	However, MPPA suggests that the term “has potential to adversely impact” may be overly broad and vague.
Central Lincoln	Disagree	Relies in the definition of Cyber System, which itself is unclear (see 1a).
NERC	Disagree	The concept of “misuse” needs to be captured along side of the current concepts of availability, degradation and compromise
Dominion	Disagree	Dominion proposes that the definition term “BES Cyber System” be changed to “Critical Cyber System” while keeping the definition text of “BES Cyber System.” This change captures the intent of the current definition, while emphasizing and clarifying the criticality of the cyber system. Dominion disagrees with the retirement of the following terms “Critical Assets,” “Critical Cyber Assets” and “Cyber Assets.” Revising the definition of the term “Critical Asset” would be superior to creating the new terms “Bulk Electric System Subsystem (BES Subsystem),” “Generation Subsystem,” “Transmission Subsystem” and “BES Cyber System.” Dominion proposes the definition of “Critical Asset” be modified to include portions of the proposed new terms “Generation Subsystem” and “Transmission Subsystem” and read: “Generation or Transmission assets (generators, substations, transmission buses, transmission lines, transformers) whose Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.” Dominion disagrees with the use of “Element” in the definitions of singular and aggregated basis. NERC currently defines the term “Element” as, “Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.” This definition would effectively apply to all electrical devices. Dominion recommends replacing “Element” with “Cyber System” as defined in Section 1.a above. As applied: (a) Singular basis – the failure of a single Cyber System would render the output of the asset unavailable; or (a) Combined/Aggregated basis - the failure of a shared Cyber System would result in the combined output of the assets becoming unavailable.
Encari	Disagree	Requirement R3.1 implies that any Cyber System within a BES Subsystem that is identified under the criteria in Attachment 1 has the potential to be a BES Cyber System. That may not be the case since the definition of a Cyber System is not tied or related to the definition of a BES Subsystem. In order to ensure the implied relationship exists, we recommend the definition of BES Cyber System be expanded to state, “A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System. A Cyber System associated with a BES Subsystem

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		identified under the criteria in Attachment 1 is presumed to be a BES Cyber System if the Cyber System has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.”
US ACE – NW	Agree	
SCE	Disagree	The definition should be revised to replace “has the potential” with “has significant potential.” The term “potential” is, standing alone, extremely broad and thus may unreasonably expand the scope of what should constitute a BES Cyber System. Including the term “significant” will help ensure that only Cyber Systems that may have a genuine impact on the BES will be within scope.
USBR	Agree	
Dyonyx	Disagree	We believe it is important that a draft of CIP-003-4 through CIP-009-4 be made available prior to the ballot requirement for CIP-002-4. This is crucial for Entities to understand the potential impact of the new classification prior to agreeing to all the criteria as specified in CIP-002-4. For example, currently the draft CIP-002-4 specifies that all BES Cyber Assets not classified as High or Medium will automatically be classified as Low. This means that those Cyber Security Controls specified in the CIP-003-4 to CIP-009-4 standards required for Low BES Cyber Assets would have to be applied. Consideration may be needed for an additional classification level of “Not Applicable” or some other form depending upon the extent of the requirements imposed by the Low classification.
FMPP	Agree	
MISO	Disagree	Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems “also includes all of the components necessary to ensure the protection of the reliability function(s) being performed”. If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
Westar	Disagree	The phrase 'has the potential to' is vague and leaves room for interpretation. Suggest replacing with 'will'.
Green Country	Disagree	A Cyber System organized to control and/or monitor the real time operation and support reliable operation of the BES.
Oregon PUC	Disagree	Oregon PUC Safety Reliability Security Staff believe the term “potential to adversely impact” has too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
NB Power Gen	Agree	However, the previous CIP-002 R3 (R3.1, R3.2, R3.3)defined criteria for classifying BES Cyber Systems such that it was clear which systems were vulnerable to remote attack and which were not. The previous set of cyber security standards addressed the vulnerability of cyber systems to cyber threats external to the facility, which seemed to be the premise for the security issue (remote coordinated attacks via communication links). If cyber systems are not connected in any way such that a threat external to the facility is neutralized, most of the rest of the CIP-003 through CIP-009 were not applicable (not required since there was no possibility for remote access attack). Most of the CIP-003 requirements made sense to implement to ensure continuous monitoring, change management and vigilance to ensure configuration

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		changes introduced no new communication links that would allow external communication to BES Cyber Systems within the facility, and to ensure that there was senior management responsibility. The revised definitions are good as far as they go, but they do change the scope of the applicability of the standards to include cyber systems that cannot be accessed from outside the facility. Within the boundaries of a generating station, whether single or multiple unit, if there are no external communication links that provide a means of access to BES Cyber Systems, whether wired or wireless, there should be no need to implement the security measures required by CIP-004 through CIP-009 for the purpose of securing the BES Cyber Systems from a remote access threat. I suggest that unless the intent has changed (i.e., now we need to protect BES cyber systems that may have impact on the BES reliability from any physical access attack within the facility instead of from remote access external to the facility) that the revised CIP-002 should include a further definition that limits the scope of applicability of the security measures to those BES Cyber Systems that have any communication link outside of the facility that allow communication to BES Cyber Systems within the facility. Alternatively, leave the definitions as currently proposed and in the other CIP Standards, allow for the isolation of BES Cyber Systems from communication access outside of the facility as a security measure that is an accepted approach to compliance. This would require appropriate documented configuration change management for ongoing vigilance.
Manitoba 1	Agree	
Wolverine	Agree	
Portland GE	Disagree	The term “potential to adversely impact” has too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
PSEG	Disagree	Comment #1: We disagree with this definition because it is not clear as to the meaning behind the phrase “adversely impact functions critical to the reliable operation of the BES”. Comment #2: A Transmission Subsystem which is identified as “Low” could not by definition have an impact on BES Cyber System (using the proposed definition)? The definition of “Low” is something that can not adversely impact the reliable operation of the BES. (Conclusion: A classification of “Low” can not have a BES Cyber System which is critical to the reliable operation of the BES.”) Comment #3: We strongly recommend that the SDT delete the word “critical” from the definition of BES Cyber System. Comment #4: We recommend that we retain the CCA terminology Comment #5: This needs to be specific to at risk cyber systems. There are cyber systems that could adversely impact the reliability of the BES that are not at risk since they do not use routable protocols. The definition of critical cyber assets was more descriptive and better suited the intent of the reliability standards. Suggestion: A Cyber System, contained within an Electronic Security Perimeter (ESP), that if compromised (through an electronic

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		interface) has the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch, relay or tap changer), interrupt a generating unit's production capability or disrupt / corrupt real-time data. Our proposed definition provides the necessary clarity as to what Cyber Systems need to be included the classification of a BES Cyber System(s). We agree with the use of the acronym Bulk Electric System (BES) for this term. This clarity is needed to reinforce that NERC's jurisdiction provided under FPA 215 includes only those facilities that fall under the definition of Bulk Electric System. Bulk Electric System as defined by NERC: "As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.
Idaho Power	Agree	
SOCO	Disagree	The phrase: "has the potential to adversely impact" is too vague. For example, a RTU could be unavailable for an extended period of time. That will be an adverse impact in that it is certainly inconvenient. However, since protection and control system operations on the BES are automatic and independent of SCADA control, loss of an RTU, for whatever reason, is not immediately or by default a critical situation. Another example is primary and secondary protective systems; the loss of one or the other but not both simultaneously is not immediately a critical situation. Suggest the following definition: A Cyber System which if rendered unavailable, degraded, or compromised will immediately impact functions critical to the reliable operation of the Bulk Electric System such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures. Suggested definition: A Cyber System which if remotely accessed and rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System or essential for the operation of a generation unit which could adversely impact the reliable operation of the BES. The phrases "essential to operations" and "routable protocol" should be added to the BES Cyber System definition.
DTE	Agree	
AEP	Disagree	In combination with the "Cyber System" definition above, this definition becomes more problematic. The Cyber System definition does not provide sufficient detail as to the level of sophistication of the devices that are at risk and that need to

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		be protected. Given that a system is made up of a collection of parts, each part does not create the same degree of impact to the BES. This draft standard collectively groups the parts, then groups the facilities, and then determines the impact of any single part based on the highest possible impact. This may well have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Disagree	See previous answer. We agree with the idea of distinguishing computerized systems that perform or support functions necessary for BES reliable operations from those that do not. However, we are concerned about how "far" or "deep" one must go in order to identify computerized systems with the "potential" to adversely impact the BES. This is not a new problem; popular examples include HVAC systems and coal conveyors that operate under computerized control. Must they be counted as BES Cyber Systems? Should business systems that play a role in Entity operations be included? The real-world answer is probably, "It depends." We believe NERC and the SDT may *have* to come down on one side or the other of this kind of question if the goal of establishing "bright lines" is to be achieved.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently.
E ON	Disagree	As described above, the definition of “Cyber System” is far too inclusive. E ON U.S. would urge the drafting team to keep in mind the purpose of the cyber security requirements, that is to prevent unauthorized electronic access to mission critical programmable devices. The re-write of CIP-002 appears to drop language in the previous versions that address assets connected via a “routable protocol.” In fact, connectivity to a cyber asset doesn’t seem to be addressed at all, leading to the concern that standalone assets, those not connected to any network, could be brought into scope through association with a high or medium rated BES subsystem. Accessing stand alone devices requires an intruder’s physical presence and connecting with proprietary interface. An intruder could far more easily operate control panel switches and thus the preventing physical unauthorized access should remain the objective. Absent the ability to remotely connect and communicate, a standalone programmable device should not be considered a Cyber Asset for purposes of these standards. There also remains ambiguity regarding network perimeter devices such as firewalls, routers, and the like. Should these devices be treated as separate perimeter devices and not part of a BES cyber system?
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	An “element” or “component” of a cyber system if compromised or not properly maintained could have the same effect.
CenterPoint	Disagree	Disagree – See comments on 1.a. This definition is very broad and would seem to describe the already accepted and understood term of a critical cyber asset.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
CA Cogen	Disagree	Our concern with Version 4 is that it removes any determination of whether a cyber asset is accessible from outside the facility. Versions 1-3 require that a cyber asset have either routable protocols or dial-up access. These limitations are important because they indicate whether the cyber asset is vulnerable. If it isn't vulnerable, then it should be treated as any other part of the equipment of the facility. These requirements for accessibility should be included somewhere in the standard. Perhaps in the global re-working of the CIP standards, they will be included somewhere else, but they could possibly be included in the definition of "BES Cyber System."
LCRA	Agree	
FRCC	Disagree	What do the terms degraded and compromised mean? They are ambiguous terms and could have many different meanings depending on who you ask. I believe there has already been an interpretation request in 2009 that sought guidance to the term degraded so this is not new. These kinds of terms should not be used in a definition or a requirement in a Reliability Standard. If the drafting team has an understanding of what they mean, they should explicitly state it and not use such ambiguous terms.
NIPSCO	Disagree	We are concerned that it is unclear as to the meaning behind the phrase “adversely impact functions critical to the reliable operation of the BES”. Suggestion: Further clarifications on the intent of this language is needed.
ConEd	Agree	
EEI	Disagree	Alternative Definition: A Cyber System, with the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch or tap changer), interrupt a generating unit’s production capability or disrupt / corrupt real-time data.
O&R	Agree	
Alliant	Disagree	We believe the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose "A Cyber System associated with the operation of a Bulk Electric System Subsystem.
Ameren	Disagree	A Cyber System should be replaced with “A Responsible Entities’ Cyber System”. To make it clear that this only includes Cyber Systems under the control of the Responsible Entity and specifically excludes entities such as Verizon. What is meant by "adversely impact"? This term could include almost anything, and needs to be more narrowly defined. We recommend replacing “has the potential to adversely impact” with “would be unable to perform”. Also, the phrase "has the potential to" needs to removed and changed to "will". We need to get away from the hypothetical and focus on the more concrete issues.
Black Hills	Agree	The definition itself is technically sound, but its implication is profound because virtually all Cyber Systems have some "potential" (unqualified) to "adversely" (unqualified) impact reliable operation of the BES.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
TNMP	Disagree	TNMP believes the Cyber System definition needs to be revised for clarity as discussed in the response to 1.a. Also the phrase “has the potential to adversely impact functions critical” lends a prejudice that a BES Cyber System has a High BES Impact. A change to “has the potential to have a high, medium, or low impact on functions critical to the reliable operation of the Bulk Electric System” would maintain the concept of potential impact while allowing for the importance to be defined by a High/Med/Low BES Impact label.
NVEnergy	Disagree	Given the remarks in 1.a above, we recommend that the term Cyber System be changed to Cyber Device or Cyber Asset.
MWDSC	Disagree	"Potential to adversely impact functions critical" is too vague. Doesn't consider systems which can be unavailable, but do not impact functions because of redundancy or other reasons.
Empire	Disagree	Option to redefine BES Cyber System to: A discrete set of one or more programmable electronic devices that operate BES devices at 200 kv and above to control and/or monitor the real time operation of the BES
NCEMCS	Agree	Not all cyber systems would have an impact. The cyber system must be in direct support of the BES or have some cascading (impact other systems that direct support of the BES) impact.
BCTC	Disagree	See Question 13
SWTC	Disagree	Not so much with BES Cyber System Definition. Here again the BES needs to be defined.
SCEG	Agree	
Exelon	Disagree	In addition to concerns about the possible overlap and or conflict between definitions used by the various regulatory entities, as the largest owner/operator of nuclear power plants in the United States we have concerns about the potential of duplication of efforts. Currently nuclear power plants employ very strict and thorough physical and cyber security controls and urge NERC to consider those protocols as the CIP standards are developed to avoid needless duplicative efforts As a result Exelon asks the SDT to consider the following revised BES Cyber System definition:. A Cyber System which if rendered unavailable, degraded, or compromised via cyber attack has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.
BPA Trans	Disagree	The Cyber System is not adversely impacting functions, its loss, degradation or compromise is. Our proposed modification would be: “A Cyber System whose compromise, degradation, or loss of availability has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.”
HQT	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” The definition is not clear, creates audit issues. Needs to be more explicit on what the definition of boundaries of cyber system applicability are. (Attachment 2 to be considered).

Organization	Yes or No	Question 1.b. Comment (Response page 6)
CCG	Disagree	Page 7 of the guidance document defines BES Cyber System and then states “This definition includes all of the components necessary to ensure the protection of the reliability functions being performed.” This addition to the definition is overly broad and inappropriate. If the definition of BES Cyber System needs to be changed to include additional components, it should be performed through the stakeholder process. There should not be additional items brought into the definition through the guidance document.
Allegheny Supply	Agree	
KCPL	Disagree	No, the definition for a BES Cyber System should not be conditional on the impact a cyber element may or may not have on the BES. This should identify the systems to be examined and the process should determine the criticality and need for appropriate security protections. I believe acceptance of this notion would effectively make the definition for “Cyber System” and “BES Cyber System” identical and, therefore, one of them could be eliminated.
Connectiv Energy	Disagree	Concerned with use of the words “potential to adversely impact…” This leaves a lot to interpretation, and if conservatively considered most cyber systems have the ‘potential’ to adversely impact a function. Adversely Impact to what degree? A minor impact may not be of concern but would meet this definition.
MidAmerican	Disagree	See comments to 1.a. on Cyber System. If Cyber System and BES Cyber System definitions are proven to be needed for categorization of security controls, the definition should be “Cyber Systems controlling BES Facilities.” This eliminates the issues of the broad, undefined concept of “potential to adversely impact functions” in the draft CIP-002-4 definition.
CPG	Disagree	For the purposes of defining a BES Cyber System, the Cyber system explanation should be combined into the BES Cyber System definition. The definition of BES Cyber System should read, “A discrete set of one or more programmable electronic devices organized for the collection, processing, maintenance, use, sharing, or communication of data, which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.” There should also be further distinction between those systems attached to routable networks and those that are not.
Santee Cooper	Agree	
OGE	Disagree	• This statement could be improved if we had something more definitive. The term "potential" is quite subjective and open to interpretation. • OPTION: A discrete set of one or more programmable electronic devices organized to control and/or monitor the real time operation of the BES.
Oncor	Disagree	Do not assume an adverse impact. Restated- “A Cyber System associated with the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
PPL Supply	Disagree	The subject definition should be clarified to exclude “market systems.” The potential inclusion of “market systems in the definition of BES subsystems and BES Cyber Systems seems to be overly broad. In general, these "market systems" allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market, among other things. An overly broad definition could end up including these "market systems" under the purview of the CIP standards which could result in increased burdens with little or no resulting increase in reliability.
St. George	Agree	
NGRID	Disagree	This definition should define what the term is, not its impact. We recommend “Is a Cyber System that directly supports the reliable operation of the Bulk Electric System” Also, the phrase “adversely impact functions critical to the reliable operation of the BES” is confusing since as per the proposed definitions of Transmission/Generation subsystems, anything identified as “low” could not by definition have a BES Cyber System, that is, a classification of “Low” can not have a BES Cyber System which is critical to the reliable operation of the BES. National Grid recommends deleting the word “critical” from the definition.
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to Cyber Systems of 100kV or greater. The use of the words “potential to adversely impact” and “critical” will leave all entities and users, owners, or operators of the BES and regulators the ability to interpret this as outside the scope of the SDT definition. Recommend that BES Cyber System read as: A BES Cyber System which if rendered unavailable, degraded, or compromised will have a direct impact on maintaining equipment or electric system’s thermo, voltage and stability limits where as instability, uncontrolled separation, or cascading failures that directly impact the reliable operation of the Bulk Electric System.
FE	Agree	
TECO	Agree	We agree with this definition, however, we do not believe the standard as currently worded accomplishes this.
CECD	Disagree	The definition references an undefined term "critical functions" which will have a significant impact on whether a Cyber Systems will be identified as a BES Cyber System, and CECD encourages the drafting team to either include a definition or a specific reference to clarify what the critical functions are or clearly state that these functions can be identified by the registered entity. In this draft, Attachment 2 entitled "Functions Critical to the Reliable Operation of the BES" is intended to define this term so there should be a reference to that Attachment if this is the direction the drafting team is taking. CECD does not agree that all of the functions described are critical (the language is too inclusive) and we would prefer to define what is a critical function for our operation, in coordination with our neighbors as appropriate.
MRO	Disagree	We feel the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose “A Cyber System associated with the operation of a Bulk Electric System Subsystem”.
GTC	Disagree	If “functions critical to the reliable operation of the Bulk Electric System” is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2.

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
Xcel	Disagree	We feel the definition should not assume an adverse impact, as that is for the processes within the standard to decide. We propose "A Cyber System associated with the operation of a Bulk Electric System Subsystem".
BGE	Disagree	We believe that for the purposes of defining "BES Cyber System" the "Cyber System" explanation should be rolled into 1.b. The definition of BES Cyber System should read, "A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System." We believe there may be further distinction required between BES Cyber Systems attached to routable networks vs. those that are not. This is because there can be a wide range of appropriate protective measures commensurate with the risks associated with those systems.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although we agree that a BES cyber system affects the reliability of the BES, this definition should include more detail on what is meant by unavailable, degraded, or compromised as there may be back-up systems to help mitigate these problems.
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	AP disagrees with this definition because it is not clear as to the meaning behind the phrase "adversely impact functions critical to the reliable operation of the BES".
FMPA	Disagree	The NERC Glossary of Terms should be used when there are defined terms available for use. Adverse Reliability Impact is such a term. Hence, the definition should read: "A Cyber System, which if rendered unavailable, degraded or compromised, has the potential for an Adverse Reliability Impact." There is no need to add the term "functions" to the definition. A results-oriented, performance based standard would simply care if there is a potential for an Adverse Reliability Impact. The addition of the concept of functions is confusing and we do not see significant added value. For instance, how are these "functions" different than the "Functional Model"?

Organization	Yes or No	Question 1.b. Comment (Response page 6)
Duke	Disagree	Definition should be revised to remove ambiguous language. Suggested wording: BES Cyber System – A Cyber System which has the potential to impact reliable operation of the Bulk Electric System.
AESI	Disagree	If "functions critical to the reliable operation of the Bulk Electric System" is intended to refer to those functions listed in Attachment 2, then it should either be capitalized and defined as a term or it should specifically refer to Attachment 2. The phrase "has the potential" is excessively vague and overly inclusive especially in conjunction with the wording of R3.2. Since requirement R3.2 mandates that all BES Cyber Assets be assigned the same impact level as their parent BES Subsystem, this phrase requires (for example) that all Cyber Systems associated with a High Impact BES Subsystem which have the potential to adversely impact … the reliable operation of the BES must be treated as High Impact, regardless of how remote the potential for adverse impact is. The term Bulk Electric System in the NERC glossary should be modified to establish a consistent definition across regions by NERC and to define the BES acronym.
IESO	Agree	
Manitoba 2	Disagree	Please define "degraded" as it applies in this definition. "Potential to adversely impact functions" should be changed to "will adversely impact functions". In the document DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems, the section "What is a Cyber System" includes "infrastructure support components – devices supporting the confidentiality, … of the BES Cyber System…" in the definition of the BES Cyber System. The primary issues to support the reliability functions are integrity and availability. Including confidentiality makes the scope of cyber systems requiring protection overly broad. It is unclear how to define the boundaries or breadth of a BES Cyber System. Are cyber systems which primarily support a maintenance activity related to a BES Subsystem to be included in the scope of this definition? If, so how is it limited to the most important activities? "Functions critical" is not defined, and should not be referenced in this definition. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	OMPA does not agree that every BES cyber system has the potential to adversely impact functions critical to the reliable operation of the BES. OMPA urges the drafting team to consider a fourth, "no impact", option for those cyber systems that do not have the potential for adversely impacting the real-time operation of the BES. This definition assumes all BES cyber systems have the potential to adversely impact the reliable operation of the BES.
ATC	Disagree	ATC disagrees with this definition because it is not clear as to the meaning behind the phrase "adversely impact functions critical to the reliable operation of the BES". A Transmission Subsystem which is identified as "Low" could not by definition have a BES Cyber System (using the

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		proposed definition)? The definition of "Low" is something that can not adversely impact the reliable operation of the BES. (Conclusion: A classification of "Low" can not have a BES Cyber System which is critical to the reliable operation of the BES.") ATC strongly recommends that the SDT delete the word "critical" from the definition of BES Cyber System. Suggestion: A Cyber System, contained within an Electronic Security Perimeter (ESP), that if compromised (through remote access) has the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (examples: circuit breaker, switch or tap changer), interrupt a generating unit's production capability or disrupt / corrupt real-time data. ATC's proposed definition provides the necessary clarity as to what Cyber Systems are to be included in the classification of a BES Cyber System(s). ATC does agree with the use of the acronym Bulk Electric System (BES) for this term. This clarity is needed to reinforce that NERC's jurisdiction provided under FPA 215 includes only those facilities that fall under the definition of Bulk Electric System. Bulk Electric System as defined by NERC: "As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.b. Comment (Response page 6)</th></tr>
<tr><td></td><td></td><td>remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>BES Cyber system: Cyber system essential to the reliable real time operation of Bulk Electric System which if rendered unavailable, degraded, or compromised has an Adverse Reliability Impact.

Adverse Reliability Impact is already a defined term in the NERC Glossary.

It is unclear whether BES Cybersystem encompasses the assess control, monitoring, and logging systems that were previously treated differently in versions 1 and 2/3 or whether they will be treated separately within the CIP-003 through CIP-009 revisions. We suggest more clarity regarding the definition of a BES Cybersystem as it could be interpreted to include HVAC, Communications systems, and even IP addressable power strips. Also the terms “potential”, “adverse” are again terms that are open for interpretation.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA proposes the following definition for BES Cyber System.</td></tr>
</table>

Organization	Yes or No	Question 1.b. Comment (Response page 6)
		BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to have an Adverse Reliability Impact to the reliable operation of the Bulk Electric System.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. The definition and consideration points used in the Guidance are more comprehensive in evaluating the various types of systems used to support reliability functions and should be the definition used. Additionally, the use of redundant components should be addressed in the definition particularly where the redundant components fully provide the same functionality of the primary system. Midwest ISO Comments: Page 7 of the Guidance Document for Categorizing Cyber Systems states that the definition of BES Cyber Systems "also includes all of the components necessary to ensure the protection of the reliability function(s) being performed". If this is the intent of the SDT this statement needs to be included in the definition of a BES Cyber System in the Standard.
PacifiCorp	Disagree	If Cyber System and BES Cyber System definitions are proven to be needed for categorization of security controls, the definition should be "Cyber Systems controlling BES Facilities." This eliminates the broad, undefined concept of "potential to adversely impact functions" in the draft CIP-002-4 definition.
PEPCO	Disagree	The draft definition is not clear and seems to be subject to interpretation. A clearer definition of - if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation. What is considered - adversely impact? What is meant by critical to the reliable operation? Does the fact that critical is used in the definition mean that it has to be a high impact system? The overall definition needs to be bright-lined. We suggest the following: BES Cyber System: An electronic cyber system with the ability to initiate (through direct command or setting adjustments) the operation of a BES switching device(s) (e.g. circuit breaker, switch or tap changer), interrupt a generating unit's production capability, or disrupt / corrupt real-time electric operations data.
NEI	Disagree	A) Clarification of the terms "degraded", "compromised", "potential to adversely impact" and "critical to the reliable operation" is required. B) NEI suggests that the definition be simplified to "A cyber system (or element or component thereof) that has the potential to impact the reliable operation of the BES." C) In combination with the proposed "Cyber System" definition, this definition becomes more problematic. The Cyber System definition does not provide sufficient detail as to the level of sophistication of the devices that are at risk and that need to be protected. Given that a system is made up of a collection of parts, each part does not create the same degree of impact to the BES. This draft standard collectively groups the parts, then groups the facilities, and then determines the impact of any single part based on the highest possible impact. This may well have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Summary Consideration: A number of respondents commented on the definitions of Subsystems (BES, Generation and Transmission), cited vagueness and suggested the use of terms already defined in the glossary and in wide use in the industry. The SDT reviewed the comments and agreed that the use of terms already defined and widely used in the industry will serve the same purpose. The definitions for Subsystems have been removed and the references in the standard use terms already defined in the NERC Glossary or in wide use by the industry and any additional clarifying terms in the standard where "subsystems" were previously used.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
Progress Energy	Disagree	NERC needs to fully define "BES Facilities" in order for this definition to be useful.
EPSA	Disagree	Current BES Subsystem definition is unclear thereby consistent identification will prove difficult. In 1.1 Aggregated Rated Name Plate and 1.2 Aggregate Output do not distinguish if the aggregate nameplate generation at a node, regardless of facility ownership or the generation controlled by a distinct control system. EPSA believes the control system can indeed have sufficient controls without every generating facility connected to it being identified as part of the Subsystem. In addition, Reserve Sharing Obligation does not distinguish whether this is for a specific Generation facility or the Balancing Authority as a whole. This is also true for Contingency Reserve.
GSOC/OPC	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say "A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center." Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
Hayden	Disagree	1. Add to the end of the sentence "...on the Bulk Electric System (>100 kv)." This is added to ensure that we are not addressing generation facilities used on distribution systems or non-BES facilities.
SDGE	Disagree	We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used in the generation or transmission of energy.
APPA	Disagree	BES Subsystem: Subsystems add an unneeded step and add confusion The SDT can get to the same classification analysis by both defining subsystems and then determining their impact on the BES, or starting directly with the worst case scenario analysis of a malicious use of a cyber system. We question the

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		purpose of adding the step of defining Subsystems to the analytical process, which seems unneeded. Since the draft does not describe how groups of Facilities are to be categorized into cyber systems, then it will be difficult to determine if the groupings developed by a registered entity are technically correct and auditable. We envision a situation where compliance authority auditors disagree with the registered entity on how Facilities are to be grouped into subsystems, without any clear requirements to guide such classifications. We also anticipate that we would get into the same situation where each entity is allowed to define its subsystems by a methodology determined by the entity. This categorization process has the potential for subjectivity that the proposed bright line criteria were intended to reduce or eliminate. We believe it is simpler, more straightforward and less confusing to skip the step of defining subsystems and simply ask registered entities to map their cyber systems' control paths to and data paths from their BES systems. This mapping is performed by asking the question: What's the worst case scenario that can be caused by a malicious use of a cyber system? What would be the "Adverse Reliability Impact" of that cyber system? If the SDT chooses to retain the concept of Subsystems, which we believe adds unnecessary complication and confusion, we recommend grouping by the scope of a Cyber System and eliminating the phrase "or ensure the ability to . . ." which is either redundant or overly inclusive of non-BES facilities. The resulting definition would read: "A group of one or more Facilities (such as a Generation Subsystem, Transmission Subsystem, or Control Center) used to generate energy, transport energy that share a common Cyber System."
Consumers	Disagree	Again, this seems to simply be another way (and again with no benefit or additional clarity) of referring to Assets. See Section 13.
NPCC	Disagree	The existing use of Facility is inconsistent with the definition in the NERC Glossary and excludes some subsystems in Attachment 1 Recommend that the definition is "one of Generation Subsystem, Transmission Subsystem, Control Center, Protection System, and SPS, RAS or automatic load shedding." Recommend this definition follow 1.f Control Center.
SWPA	Disagree	The use of the term "ensure" in this context is improper. It is not possible to "ensure" that the thousands upon thousands of mechanical parts which make up the BES will continuously be available for the generation or transportation of energy. This is simply beyond the ability of any registered entity. Suggest replacing with "A group of one or more BES facilities controlled and/or monitored by a common BES cyber system."
MPPA	Agree	Language could be added to more clarify that these standards apply to those systems above 100 kv.
Central Lincoln	Disagree	Definition relies on the definition of the BES, which is not understood and is inconsistently interpreted across the regions. Continuing to use a flawed definition to define others only increases the ambiguity. Suggest NERC and/or the regions finish the BES definition work before building further on top of it.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		Suggest removing the word “system”, so that we don’t have the redundant “system subsystem” in the defined term.
Dominion	Disagree	See comments to 1.b.
Encari	Disagree	We further recommend that “BES Subsystem” refer to asset types with minimal thresholds for materiality. For example, “generation plant” could be replaced by the term, “generation resource that meets the criteria for inclusion in the NERC compliance registry.” Absent materiality thresholds, a SCADA system that controls two wind powered generator units, each at separate locations, with a combined generation capacity of 10,000 kWh annually, could be considered a control center.
US ACE – NW	Agree	
SCE	Agree	
USBR	Agree	
Dyonyx	Disagree	The structural intent of the BES Subsystem, Generation Subsystem, Transmission Subsystem, and Control Center terms conceptually appears to be quite appropriate. However, the definition of the terms “used in the definitions” is very confusing. First, the term “BES Subsystem” itself is a confusing use of the word “subsystem”. The proposed definition for the “BES Subsystem” uses the phrase a “group of one or more BES Facilities….” Why not go ahead and use the term “BES Facility” and define it as “A group of one or more Generation Subsystems, Transmission Subsystems, or Control Centers used to generate, transport energy or ensure the ability to generate or transport energy”? The use of the recommended term “BES Facility” is a separate definition from “facility” in the NERC Glossary of Terms and in our opinion the former is more appropriate for use herein.
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to ensure the ability to generate or transport energy.
Oregon PUC	Disagree	The term “ensure the ability to generate or transport energy” is too broad and leaves too much room for auditor and enforcement interpretation. Clear, specific and technically defensible language is needed for this definition.
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	The term “BES Facilities” needs to be defined.
PSEG	Disagree	Comment #1: The terms Generation Subsystem, Transmission Subsystem and Control Center seem to provide the

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		necessary granularity to effectively convey the SDT intentions of this definition. We believe that this definition is not required and therefore should be deleted. Comment #2: We are concerned about the use throughout these documents of the words Facilities, Elements, and subsystem. These do not appear in the glossary and in some cases appear confusing and potentially conflict with those interpretations used in other NERC standards: TPL, FAC, EOP, etc.
WE-Energies	Disagree	The definition of BES Subsystem includes the vague statement “or ensure the ability to generate or transport energy." This is unnecessary and should be deleted.
Idaho Power	Agree	
SOCO	Agree	
DTE	Disagree	Since this term is used in the standard as a combination of the next three terms, Generation Subsystem, Transmission Subsystem, and Control Center consider changing it to the following to avoid repetition and confusion. Bulk Electric System Subsystem (BES Subsystem) — A Generation Subsystem, Transmission Subsystem, or Control Center.
AEP	Disagree	Defining groups of BES facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Disagree	The structural intent of the BES Subsystem, Generation Subsystem, Transmission Subsystem, and Control Center terms conceptually appears to be quite appropriate. However, the definition of the terms “used in the definitions” are very confusing. First, the term “BES Subsystem” itself is a confusing use of the word “subsystem”. The proposed definition for the “BES Subsystem” uses the phrase a “group of one or more BES Facilities….” Why not go ahead and use the term “BES Facility” and define it as “A group of one or more Generation Subsystems, Transmission Subsystems, or Control Centers used to generate, transport energy or ensure the ability to generate or transport energy”? The use of the recommended term “BES Facility” is a separate definition from “facility” in the NERC Glossary of Terms and in our opinion the former is more appropriate.
Calpine	Agree	
NS&T	Disagree	We believe the goal of allowing flexibility in how Entities define their "BES Subsystems" has resulted in a definition with too many degrees of freedom, and that the result could be disproportionate amounts of time spent on how to draw "subsystem" lines around BES assets, to the detriment of improving cyber security.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently.
E ON	Disagree	After reviewing Attachment 1, E ON US surmises that the category "ensure the ability to generate or transport energy" refers to Control Centers. E ON U.S. recommends it be stated as Control Centers to avoid ambiguity.
Carthage		CWEP would like better clarification on BES Subsystems. Is the standard referring to the BES as defined in the NERC Glossary? If so, are entities with no facilities or assets that operate at 100 kV and higher meant to be exempt?
WECC	Disagree	Not sure that we need this additional level of definition. Something is either part of the BES or not and it is redundant with the definition of generation, transmission, and control center following.
Entergy	Disagree	Doesn't translate well in practical terms to aid Entities identify what needs to be protected. Examples: How do cranking paths translate into "subsystems" and/or "facilities?" Generation-Transmission interconnection methods vary widely, not always including a "switchyard" per se, and are often comprised of assets owned/operated by more than one Entity – how do the various scenarios equate with subsystems and/or facilities? What about special protection schemes – subsystems and/or facilities? These challenges in definition highlight the incongruity in attacking the issue of cyber security using primarily a grid electrical engineering frame of reference versus that of networked computing systems engineering. Square peg, round hole.
CenterPoint	Disagree	Disagree – See comments on 1.a and 8. This definition could create auditable implementation confusion due to the interconnected nature of the BES. For example, ten power plants could be a "subsystem", or could represent two "subsystems" of five power plants each, or three "subsystems" adding up to the ten power plants, or various other combinations. Alternatively, the ten power plants plus "connecting" transmission assets (which could be defined in multiple ways since the entire BES is interconnected) could be a "subsystem". Moreover, subsystems that "ensure the ability" to generate or transport energy could be construed in multiple ways to include or not include such things as fuel pipeline systems, for example. Since a pipeline system is generally a common carrier system outside the control of the responsible entity, the question then becomes how many of the pipeline assets should be construed as the "BES subsystem"? In short, the proposed definition creates confusion without appearing to add anything of value.
LCRA	Agree	
FRCC	Disagree	I do not believe that the definition helps and in fact if you look at R1 where the application of the criteria in attachment 1 is required, you really do not need to have the definition of BES Subsystems. The criteria are pretty clear and this definition does not help.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility within the proposed definitions.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
ConEd	Agree	
EEI	Disagree	Differentiating between high, medium and low Bulk Electric System Subsystem may have little value or credibility for associated cyber security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
O&R	Agree	
Alliant	Agree	
Ameren	Agree	None
Black Hills	Disagree	The definition (size-wise) of what must constitute a "subsystem" is not defined, and therefore would be relative to the interpretation by the entity (some of which could be very large or very small).
TNMP	Disagree	Using the phrase “a group of one or more BES Facilities” permits multiple possible constructs of BES Subsystems owned by a Responsible Entity. A BES Subsystem could be a comprised of a number of substations along a critical path transmission path or cranking path. If the drafting committee is looking to move forward with the concept of ”one or more BES Facilities” then a better definition or criteria of when it applies to multiple BES Facilities is needed to give the standard “bright lines”. Also, the definition refers to “BES Facilities,” but neither the proposed standard nor current NERC glossary contain this term. Either the phrase needs to be officially defined or removed from the definition.
NVEnergy	Agree	
MWDSC	Disagree	Unclear whether the term "BES" has been accepted as a NERC defined term instead of "Bulk Power System". What about regional differences in defined BES? A BES Subsystem may be isolated and not affect other interconnected systems. For example, if you have one generator with a radial line to a load, it wouldn't affect any other system. Wouldn't the standard require a "low impact" assessment with unknown cyber security measures?
Empire	Disagree	Optional definition: BES Subsystem: A group of one or more BES Facilities controlled and/or monitored by a common BES Cyber System
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	The definition of a BES Subsystem again goes back to what is the BES.
SCEG	Agree	We agree with the definition, however we feel that the SDT needs to ensure that any subsystem which does not meet one of these three defined categories is defined.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
Exelon	Agree	Although Exelon agrees with this definition, as stated previously Exelon has concerns with the proposed CIP standard definitions that may result in overlaps and/or conflicts in definitions between the regulatory entities (NRC, CNSC, and NERC). We ask that NERC and/or the SDT take action to ensure the proposed definitions are reviewed and revised if needed to eliminate any potential overlaps. In addition Exelon is hoping for a timely and clearly stated scope of applicability from the NRC to U.S. nuclear plant owners/operators. As currently drafted the system/subsystem concept and the Attachment 1 criterion without the scope of applicability will likely create confusion as NERC and the SDT attempt to define the standards. The industry will likewise have difficulty as they attempt to understand and comply with the CIP standard requirements.
BPA Trans	Disagree	The term “BES Facilities” needs to be defined.
HQT	Disagree	The existing use of Facility is inconsistent with the definition in the NERC Glossary and excludes some subsystems in Attachment 1 Recommend that the definition is “one of Generation Subsystem, Transmission Subsystem, Control Center, Protection System, and SPS, RAS or automatic load shedding.” Recommend this definition follow 1.f Control Center The standards are written as if there is one easily defined set of BES Subsystems. This is not the case. From the cyber perspective alone there could be a different set of BES Subsystems for each type of cyber subsystem.
Allegheny Supply	Agree	
KCPL	Disagree	No, with appropriate definitions for the Generation and Transmission Subsystem, this is redundant and does no more to advance the clarity and focus of the CIP Standards to identify the components and physical facilities under consideration for cyber protection.
Connectiv Energy		
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13. This definition is not needed at this time. The necessity of this definition is caused by CIP-002-4’s proposed framework to use categorization of “iron” (substations and generating units) to categorize security controls for Cyber Assets, which are very different from “iron.” If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time, including the relevance of the associated Attachment 1. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
CPG	Disagree	This definition is not needed as the Generation, Transmission, and Control Center definitions are sufficient by themselves.
Santee Cooper	Disagree	It would seem to suggest that a BES Subsystem is a category underneath the BES Cyber System. Why not define the BES at a higher level, and forego the BES Subsystem.
OGE	Disagree	• Please provide a definition of "shared element". • What is the definition of Bulk Electric System Subsystems for generation plants and transmission systems? Can you provide examples? • OPTION: A group of one or more BES Facilities controlled or monitored by a common BES Cyber System. • The terms "transport energy" should be "transport electricity"
Oncor	Disagree	BES Subsystem appears to be a term used elsewhere in the standard to refer to Generation Subsystem, Transmission Subsystem or Control Center. If this is true, restate- "refers to Generation Subsystem, Transmission Subsystem and/or Control Center."
PPL Supply	Disagree	Please see comment in response to question 1.b.
St. George	Disagree	Every BES Facility should be specifically listed to avoid ambiguity.
NGRID	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center provide the necessary granularity to effectively convey the SDT intentions of this definition. National Grid believes that this definition is not required and therefore should be deleted. BES Electric System does not align with the terms (transmission/generation subsystems) used in Attachment 1. Also, other subsystems mentioned in Attachment 1 - Protection System, SPS will usually fall under Transmission/Generation subsystems so there is no need to mention them as "subsystems".
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to BES Subsystem(s) of 100kV or greater and the three components that that make up the BES Subsystem (Generation Subsystem, Transmission Subsystem, and Control Center). This definition is not required and should be removed since Generation Subsystem, Transmission Subsystem, and Control Center are clearly defined.
FE	Agree	
TECO	Agree	

Organization	Yes or No	Question 1.c. Comment (Response page 7)
CECD	Disagree	One of the defining lines for determining if an entity is a BES user, owner or operator is whether the equipment is operated at 100 kV or above. A generation subsystem or a transmission subsystem has one line diagrams by which the connectivity can be evaluated. A control center is more appropriately considered a Cyber System to be evaluated in relation to BES Generation or Transmission Subsystems. CECD is in favor of supporting a definition of BES subsystem that keeps enough flexibility for the registered entity to define their BES subsystems, including the ability to exclude a control center as a BES Subsystem.
MRO	Agree	N/A
GTC	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say “A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center.” Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
Xcel	Agree	
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. We recommend the following definition: Bulk Electric System Subsystem (BES Subsystem) A group of one or more BES Facilities (i.e., Generator, generator step-up transformer, transmission line, substation transformer, bus(es), and associated switches, breakers, capacitors, reactors, static var compensators, transmission control center, generator control center, market operations center used to generate energy, transport energy or ensure the ability to generate or transport energy.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center seem to provide the necessary granularity to effectively convey the SDT intentions of this definition. AP believes that this definition is not required and therefore should be deleted.
FMPA	Disagree	The process laid out in the standard is to group Facilities into “BES Subsystems”, then define the impact of that subsystem while considering the functionality of the control systems and BES subsystems. FMPA believes this whole process to be more complicated than necessary and fraught with ambiguity in defining subsystems and functions. FMPA believes these steps are unnecessary and we can get to the same point by asking ourselves “what is the worst case contingency / scenario that can be caused by malicious use of a cyber system” and use this worst case analysis against the High, Medium and Low impact framework laid out by the SDT. By doing so, we eliminate the need to define subsystems and functions.

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		An example of ambiguity in the concept of subsystems is how are Facilities grouped into subsystems? Are responsible entities supposed to develop subsystems of any combination (e.g., an almost infinite variety) of Facility groupings? Do the Elements have to be connected to each other? Do they have to be all controlled by the same cyber system? Is there opportunity for disagreement between the entities and compliance enforcement on the definition of subsystems? So far, no one has been able to tell us clearly what a subsystem is, so, that is telling in and of itself. If the SDT insists on retaining the concept of subsystems, then this ambiguity needs to be clarified. For instance: “A group of one or more Facilities used to generate energy, transport energy or ensure the ability to generate or transport energy that share a common Cyber System.” Also, for clarity, the terms BES Subsystem and BES Facility are redundant. The NERC Glossary defines a Facility as: “(a) set of electrical equipment that operates as a single Bulk Electric System Element;” hence, by definition, a Facility is part of the BES. And, since a BES Subsystem is a grouping of Facilities, which by definition are part of the BES, then the Subsystem by definition is part of the BES and the term can be simplified to “Subsystem”.
Duke	Disagree	Definition should be revised to remove ambiguous language. Suggested wording: Bulk Electric System Subsystem (BES Subsystem) – A group of one or more BES Facilities (i.e. Generation Subsystem, Transmission Subsystem, and Control Center).
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	"Facility" is defined in the NERC Glossary as operating as a Bulk Electric System Element, so "BES" here is redundant. We suggest the definition be changed to simply say “A generic term for a Generation Subsystem, Transmission Subsystem, or Control Center.” Any additional specificity should be in the individual subsystem definition. Although a generic term may be useful in some context, any actual standards that are developed should be specifically applicable to either a Generation Subsystem or a Transmission Subsystem or a Control Center.
IESO	Disagree	Replace the word "energy" with the word "electricity". The word energy is too broad for the scope of these standards. The word electricity is also consistent with the term BES.
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	OMPA is concerned that the draft guidance for the electric sector paper allows the definition of BES subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. This could lead to subjectivity; specifically with respect to the auditing process and auditor interpretation. OMPA prefers mapping control and data paths from identified BES systems.
ATC	Disagree	The terms Generation Subsystem, Transmission Subsystem and Control Center provide the necessary granularity to effectively convey the SDT intentions of this definition. We believe that this definition is not required and therefore should

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.c. Comment (Response page 7)</th></tr>
<tr><td></td><td></td><td>be deleted.</td></tr>
<tr><td>LES</td><td>Agree</td><td>
We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to
</td></tr>
</table>

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
PSE	Agree	
IMPA	Disagree	IMPA recommends the replacement of the word "ensure" with the words "assist in". The word ensure means "to make certain, sure, safe – guarantee". There is no guarantee that with a Control Center in place, utilities will have the ability to generate or transport energy. A Control Center can assist with these functions but cannot ensure them.
ERCOT	Disagree	Request clarification if this grouping may span multiple locations. BES Facilities is not a defined term and should not be capitalized as such.
PacifiCorp	Disagree	See PacifiCorp's summary comments in question 13. This definition is not needed at this time. The necessity of this definition is caused by CIP-002-4's proposed framework to use categorization of "iron" (substations and generating units) to categorize security controls for Cyber Assets which are very different from "iron." If it is required in order to categorize high, medium or low security controls for discrete Cyber Assets, it should be defined when the security controls are developed. The accuracy of the definition can be assessed meaningfully at that time, including the relevance of the associated Attachment 1. PacifiCorp submits that the security controls work must be completed to determine what categorizations are possible and needed. PacifiCorp has reviewed the existing controls and observes that many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points.
PEPCO	Disagree	We suggest the following: BES Subsystem - A group of one or more BES Facilities (i.e. BES Generation Subsystem, BES Transmission Subsystem, and/or BES Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.
NEI	Disagree	A) Simplify to state "A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) B) Need to define what constitutes a "group" C) Doesn't aid Entities in identifying what needs to be protected, and, where assets are owned by more than one entity,

Organization	Yes or No	Question 1.c. Comment (Response page 7)
		how do the scenarios translate to subsystems or facilities, or the protection methodologies required? D) Defining groups of BES facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it may vary significantly with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Summary Consideration: A number of respondents commented on the definition Generation Subsystem, cited vagueness and suggested the use of terms already defined in the glossary and in wide use in the industry. The SDT reviewed the comments and agreed that the use of terms already defined and widely used in the industry will serve the same purpose. The definitions for Subsystems have been removed and the references in the standard use terms already defined in the NERC Glossary or in wide use by the industry and any additional clarifying terms in the standard where "subsystems" were previously used.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
Progress Energy	Disagree	Remove "shared element or" from definition since these CIP standards are only intended to improve protections around cyber security assets.
EPSA	Agree	EPSA generally supports the definition and use of Generation Subsystem. However, the SDT is encouraged to formally define "shared element" and "shared Cyber System." The use of shared in this definition does not specify physical, ownership or other intangibles that could constitute shared elements.
GSOC/OPC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with "including generation units" is unclear; if the intent is to say that "multiple generation units whose combined output etc" must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase "shared Cyber System" is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Hayden	Disagree	1. Change the first line to read "Generation plants, or generation units including Facilities required to connect them to the Bulk Electric System (BES), singularly or in..." This is to emphasize that the focus is on the BES and not on distribution systems.
SDGE	Disagree	We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: Generation plants or generation units, including the Facilities required to connect them to a transmission system.
APPA	Disagree	APPA Task Force Comments:

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		See Comment for BES Subsystem. No comments on the SDT's proposed definition if this approach is adopted.
Consumers	Disagree	There is no need to introduce this term. The NERC Guide already addresses this as "common mode" failure. See Section 13.
NPCC	Disagree	Definitions should not include impact. Recommend the following definition - Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination.
MPPA	Agree	
Central Lincoln	Disagree	Don't see how the part past the final comma adds anything to the definition. Who decides whether each unit within the plant or the plant itself constitutes a subsystem and how? Although the guidance document states the level of granularity is up to the registered entity, the draft standard does not make this statement. We think the SDT meant generation subsystems to be a subset of the BES subsystems. The proposed definition does not state this, though, and roof top photovoltaic systems may unintentionally be included.
NERC	Disagree	1. The concept of "misuse" needs to be captured along side of the current concepts of availability, degradation and compromise; 2. The definitions and application of Transmission Subsystems and Generator Subsystems provides the opportunity for artificial behavior in categorizing impact levels. The categorization process could drive entities to de-couple cyber systems that support multiple assets within an existing subsystem in order to classify them as different subsystems, each with a corresponding lower impact level. Those actions can result in additional security weaknesses and possibly impact the reliable operations of the subsystem.
Dominion	Disagree	See comments to 1.b. In addition to those comments, Dominion suggests that if the term "Element" is used in the context of cyber security, then greater specificity be added to the definition of "Element."
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	This definition needs to be tied back to the BES registration requirements. The Definition should be modified to reflect that the elements are components of a BES facility. The word "BES" needs to be inserted as follows: BES Generation Subsystems

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		BES Generation plants The words “of a BES” need to be inserted after “generation units”. The last part of the sentence should be deleted as it does not add to the definition by implying that a loss of generation facility output could compromise its control. The words “including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System” should be deleted. The SDT should carefully evaluate the need to use this term. It creates an overlap with the new definition proposed by the SDT for BES Subsystems. The language in this standard could easily rely on BES systems when it intends to refer to generation facilities and then restrict Generation Subsystems to aggregate or singular generating units. That would fit better with Attachment 1.
Dyonyx	Disagree	The use of the terms “Facility” in the context of this CIP Reliability Standard in defining “Generation Subsystem” is complicated by the convoluted nature of the definition of the former terms (“Facility” and “Element”) in the current NERC Glossary of Terms and extends the confusion accordingly. Also, will there be any mention of the need to consider units and facilities less than 20 MW and 75 MW respectively?
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	Generation plants, comprised of single generation units or in combinations of units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.
Oregon PUC		No comment
NB Power Gen	Disagree	Perhaps the definition would be clearer if there were two sentences. The phrase "...including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System." could be a separate statement within the definition. E.g., A Generation Subsystem also includes generating units or facilities having any shared element or cyber system whose loss or compromise may cause the combined output to become unavailable.
Manitoba 1	Agree	
Portland GE	Disagree	We propose: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination.” Delete everything after “combination” in the third line.
PSEG	Disagree	Comment #1: Concerned about the use throughout these documents of the words Facilities, Elements, and subsystem. These do not appear in the glossary and in some cases appear confusing and potentially conflict with those interpretations used in other NERC standards: TPL, FAC, EOP, etc. Comment #2: There is no need to introduce this term. The NERC Guide already addresses this as “common mode”

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		failure.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard. In addition, Wisconsin Electric Power Company has the following comments: The text "… including the Facilities required to connect them to a transmission system …" may cause an entity to secure or enclose all generating facilities' transformers and switch yards, which may not be the intent of the standard. We will need further clarity for " … shared Cyber System …". For example, if each generation plant distributed control system has its own network and can operate when disconnected from the common and high level network, is the loss or compromise of these shared elements have to be considered?
Idaho Power	Disagree	Need to define element. It would be helpful to provide some examples of what might constitute a shared element.
SOCO	Disagree	This definition extends beyond the scope identified in the purpose as stated on page 4 of the Standard. The Standard is intended to categorize "BES Cyber Systems" and this definition appears to extend into the area of "physical systems". The use of the word "element" would indicate that a manually controlled conveyor, or even a rail system, providing fuel to multiple generation units would be subject to categorization. The loss of these "elements" could impact plant operations over an extended failure period, but may not be subject to a cyber event. The words "Generation plants" should be removed. It adds no additional value, "Generation Units" and their facilities identify a clearer subsystem. The word "Facilities" should be replaced with "supporting subsystems" to indicate equipment vs. an entire plant site. Suggested definition Generation units including the supporting subsystems required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared Cyber System.
DTE	Agree	
AEP	Disagree	Defining groups of generation facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
Edison Mission	Disagree	The use of the terms “Facility” in the context of this CIP Reliability Standard in defining “Generation Subsystem” is complicated by the convoluted nature of the definition of the former terms (“Facility” and “Element”) in the current NERC Glossary of Terms and extends the confusion accordingly.
Calpine	Agree	
NS&T	Disagree	See previous comment on BES Subsystem. The common "shared Cyber System" criterion could compel the process of identifying "Generation Subsystems" to be iterative and, as a result, inordinately time-consuming. We urge the SDT to strive for a simpler and more concise definition for the sake of consistency across multiple Entities and Regions, and also to allow finite resources to be applied to the most important task = improving cyber security. We believe, in addition, this would serve the goal of being able to perform audits in an efficient and consistent manner across the various Regions.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently. Also, if used should only apply to generation over 25 MW nameplate per GO/GOP criteria.
E ON	Disagree	Because nearly all generating units are tied into SCADA/EM systems the definition appears to allow for any combination of a registered entity’s generating units from all units to any number/combination of less than all units. In order to comply an entity would need to classify every conceivable combination, or remove units from SCADA/EM systems. It is unclear whether the term ”Facilities” refers to the Facilities identified in FAC-008/009.
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	On November 16, 2009 NERC issued the “Final Report from the Ad Hoc Group for Generator Requirements at the Transmission Interface” defining what is considered part of ‘generation’ and what’s part of ‘transmission’ in different interface scenarios. This definition does not embrace the granularity of that guidance.
CenterPoint	Disagree	Disagree – See comments on 1.a, 1.c, and 8. However, some of the concepts in this proposed definition, such as the concept of shared elements or cyber systems, could possibly be added to CIP-002-2 - R1.2.3 for additional clarification.
LCRA	Agree	
FRCC	Disagree	See comment to question 1.a.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility and element within the proposed definitions.
ConEd	Disagree	Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		facilities.
EEI	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective. We suggest: Generation Subsystem — Generation plants, protection systems, or generation units including the Facilities required to connect them to a transmission system, generation units whose combined output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.
O&R	Disagree	Comments: Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
Alliant	Disagree	We believe the definition needs to be reworded as noted below for clarity: "BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss of compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem." Please clarify "shared." The terms "generation plant", "generation unit", and "transmission system" need to be defined in the NERC Glossary of terms.
Ameren	Disagree	This definition is too vague and confusing. The phrase “singularly or in combination” brings significant uncertainty as to the intended objective. What is the definition of “shared element”? This needs to be a defined term.
Black Hills	Disagree	Need to identify that this is a subset of the BES Subsystem definition. Might be better to stop the definition after the word 'combination'. Concern that the subsequent qualifiers ("whose combined output") could make separate generators (too small to even be registered with NERC) to be affected by this definition because of a "shared element or shared Cyber System". "element" should be "Element".
TNMP	Disagree	TNMP sees this definition as satisfactory. It accomplishes the intention of defining a Generation system without being overly broad and is properly constrained even with the inclusion of “Facilities required to connect”. When one looks at the NERC definition of Facilities it is clear that it is limited to discrete elements (e.g. lines, transformers) not an entire switching station. The connection would be to a Transmission Subsystem, thus, the R2 requirement of the proposed standard.
NVEnergy	Disagree	Some clarity is warranted with this definition. For instance, what constitutes the “transmission system” in the context above? We would assume that this is the point of connection of the Generator Step Up transformer to the high voltage bus, but this could be interpreted to include an entire transmission switching station if not clarified otherwise. This definition is overly broad for a “subsystem”. The description here more accurately describes an entire Generation

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		System. We believe there needs to be some constraint in this definition on a locational basis within the BES. Suggested language: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination if their combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.”
Empire	Disagree	Optional definition: A group of one or more generation units controlled and/or monitored by a common BES Cyber System.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Disagree with Cyber System Definition in 1a.
SCEG	Disagree	This definition could, in the extreme interpretation, be problematic because of the phrase "or shared Cyber System." If that phrase is struck from the end of the sentence, the definition is fine. Strictly interpreted by the definition, one physical access control system that controls access to the facilities at all of the power plants would mean that they become one generation subsystem. In other words, all of the generation plants/units attached to any BES cyber system would become a single Generation Subsystem. This seems to contradict wording in the proposed standard that contemplates more than one subsystem connected to a single cyber system. It says in R3.2: "Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."
Exelon	Disagree	Exelon has concerns that the proposed definition may be open ended and subject to vastly differing interpretations (e.g. singularly or in combination) and suggest the following revisions: Generation Subsystem — Generation plants, or generation units at a common site including the Facilities required to connect them to a transmission system, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared BES Cyber System.
BPA Trans	Disagree	We propose: “Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination.” Delete everything after “combination” in the third line.
HQT	Disagree	Definitions should not include impact Recommend the following definition - Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination.
Allegheny Supply	Agree	Generation Subsystem – the term “shared element” in the “Generation Subsystem” definition is too broad and needs clarification. This term is critical to the definition of a “Generation Subsystem”. (e.g. This definition could be interpreted to mean that all generation is a single “Generation Subsystem” because is has the transmission system as a shared

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		element.)
KCPL	Disagree	No, this definition should limit itself to the generation facility itself. The terms, “shared element or shared Cyber System” are too vague as to what that represents and, again, makes this definition conditional. The CIP standard should identify the facilities to be included for evaluation (as this is attempting to do) and allow the process for determining the impact a facility or facilities has on the BES to drive the appropriate level of cyber protection.
Connectiv Energy	Agree	One concern is that “Shared Element…” would be defined to include a Transmission Owner’s asset (farther up the line from a single plant connection) to which generating units from more than a single GO are attached? In this case would NERC look to aggregate generation from more than a single GO which singularly might not be part of the BES but due to their “Subsystem” connection could force them into the BES due to the combined total generation? This would not be desirable.
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13 and comments on BES Subsystem above in 1.c. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the “iron” (generating unit) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase “singularly or in combination.” If the definition is needed, it should refer to the distributed control systems for BES generating units in scope. New NERC Glossary definitions must carefully consider for impacts to other NERC standards.
CPG	Disagree	This definition of Generation Subsystem should clearly identify that it includes all equipment from the point of interconnection to the generating unit(s). Facilities required to connect them to the transmission system could mean a bus, a transformer, a switch, a breaker, and so forth. It is too broad.
Santee Cooper	Agree	
OGE	Disagree	• Provide clarity on your definition of a "shared element" and "shared Cyber System". Fuel source? Water Source? Train Tracks? • Adequate detail is required to avoid incorrect interpretations by all parties. • What is the purpose of the last part of the definition, “…including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System…”? It seems as though that is a subset of what has already been described by the first part of the definition. • What level of output from a single or combination of unit that would affect the Bulk Electric System? • OPTION: A group of one or more generation units controlled or monitored by a common BES Cyber System. Once clarity is achieved for what is meant by “common BES Cyber Systems”.
PPL Supply	Disagree	Comments: Agree with EEI comment that the definition can be unclear. However, removing “singularly or in combination,”

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		as proposed by EEI does not improve the clarity. In addition EEI's proposed definition adds "protection systems", which does not seem to be appropriate for the definition of generation sub-system. Protection systems should be considered and evaluated as Cyber Systems. We propose the following definition: Generation plants, or generation units (singularly or in combination), including the Facilities required to connect them to a transmission system, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.
St. George	Agree	
NGRID	Disagree	National Grid believes that the definition should not include impact and propose the following definition "Generation plants or generation units including the Facilities required to connect them to a transmission system, singularly or in combination. Generation units sharing an element or Cyber System must be additionally categorized in combination".
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to a Generation Subsystem(s) connected at 100kV or greater. Many entities are not vertically integrated where they do not own the generator and transmission elements collectively. As written, a GO may be responsible for TO Facilities. A GO may not have the understanding of the limitations and capabilities of a TO Facility. Please clarify. As written please clarify what a "shared element" is since "Element" is not capitalized as in question 1.e. Recommend rewriting to include "shared cyber element", this will clearly define the intent of the definition. Refer to question 1.a. concerning a shared "Cyber System". As written if there is no "shared element" then the stand alone generator connected at 100kV and above is not a Generation Subsystem. Please clarify what a "shared element" refers to. Is this a cyber element that is common to two generators or could this be a non cyber physical element? Recommend that physical elements (non cyber) not be covered by CIP Standards. Please clarify if the definition is attempting to identify Generation plants/units including Facilities and their components (breakers, RTUs, unit control systems) or the cyber protection systems that guard against cyber attacks. Recommend that Generation Subsystem definition be rewritten to clearly define what a Generation Subsystem is. Recommend the definition to read: "Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination". The remaining proposed SDT definition should be added to Attachment 1 since the intent seems to be a sub component of what the intent of the definition actually is trying to state.
FE	Disagree	The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System".

Organization	Yes or No	Question 1.d. Comment (Response page 8)
TECO	Disagree	We support EEI's comment and suggest the following changes to the proposed definition. Generation Subsystem — Bulk Electric System Generation plants, protection systems, or generation units including the Facilities required to connect them to the Transmission Subsystem, generation units whose combined output could become unavailable due to loss, compromise, or significant degradation of shared BES Cyber System.
CECD	Disagree	The definition should be modified as follows: Generation plants or generation units, including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System.
MRO	Disagree	We feel the definition is ambiguous as written, and propose the following reworded definition for clarity: BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss or compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem. We also would like a clarification of "shared" as we had disagreement just within our MRO NSRS group on what this term implied. Regardless, the terms "generation plant", "generation unit", and "transmission system" should be defined in the NERC Glossary of Terms.
GTC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with "including generation units" is unclear; if the intent is to say that "multiple generation units whose combined output etc" must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase "shared Cyber System" is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Xcel	Disagree	We feel the definition is ambiguous as written, and propose the following reworded definition for clarity: BES generation plants, including the Facilities required to connect them to a transmission system. Generation units whose combined output could become unavailable due to loss or compromise of a shared generation Element or shared generation Cyber System shall be considered as a single Generation Subsystem. We also would like a clarification of the term "shared". The terms "generation plant", "generation unit", and "transmission system" should be defined in the NERC Glossary of

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		Terms. The Standard needs to include a clarification where remote generation assets controlled from one plant can also be treated as multiple units at a plant facility. I.e.: Plant site has four units, no shared connectivity, same thing for remote plant/unit if the controls are independent from the controlling plant controls.
BGE	Disagree	The last term of item 1.d. should be “BES Cyber System”, not “Cyber System”, since we recommended the removal of the definition of “Cyber System”. The term, “shared element” is vague and may include items unrelated to cyber security. We recommend that the term “shared element” be omitted. We recommend the following definition: Generation Subsystem — Generation plants, or generation units, including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System. Communication networks and data communication links between discrete BES cyber systems need not be considered as a “shared cyber systems” in the determination of facilities that constitute BES Subsystem. Even with this modification, we are concerned that the definition is overbroad in that there is no limit to combining disparate systems and considering them a single subsystem.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective.
FMPA	Disagree	As discussed above, there is no need for adding the concept of Subsystems. Also, FMPA does not see a reason to define Generation, Transmission and Control Center Subsystems separately, which can introduce opportunities for confusion and for the definitions to conflict with each other. FMPA recommends eliminating the concept of subsystems. Failing that, we would recommend eliminating the sub-sub-systems of Generation, Transmission and Control Center subsystem. Failing that, if the SDT insists on retaining this concept, the definition is confusing and complicated and could be greatly simplified by: “Generation and associated Facilities that share a common Cyber System” We fail to see why sharing a common Element is important to this standard. If it is a common mode failure that the SDT is concerned about, that will already be captured in the criteria for any Cyber System that controls that shared Element. The purpose of the standard is to determine which Cyber Systems’ cyber security to regulate, so, if the SDT decides to keep the unnecessary concept of Subsystems, they should not be determined by shared elements, but by shared Cyber Systems.

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		Again, the NERC Glossary of Terms should be used when appropriate and the word “Element” should be capitalized (for clarity, we should never use a non-capitalized word that is in the NERC Glossary); however in this case the more appropriate term should be “Facility” since it is part of the BES. Note also that we should be consistent with using BES as an adjective. If the SDT chooses to retain the unnecessary concept of Subsystems, then the SDT ought to either rename this “BES Generation Subsystem”, or rename “BES Subsystem” as just “Subsystem”.
Duke	Disagree	This definition should be revised to clarify that a control room for a multiple unit site would be part of the site, and would not be considered a Control Center. Suggested wording: Generation Subsystem – Generation plants, or generation units including the facilities up to the point of interconnection with the transmission system.
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including generation units” is unclear; if the intent is to say that “multiple generation units whose combined output etc” must be treated as a single Generation Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition since individual generation units would already be considered Generation Subsystems. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
IESO	Agree	
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.d. Comment (Response page 8)</th></tr>
<tr><td></td><td></td><td>efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Generation Subsystem — Generation plants or units as identified in the Registration Criteria including the Facilities required to connect them to a transmission system, BES protection systems, and generation units whose combined output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.</td></tr>
</table>

Organization	Yes or No	Question 1.d. Comment (Response page 8)
IMPA	Disagree	This definition is not very clear on how a generation plant needs to be classified if it has more than one generating unit. It is not clear how to classify multiple units that are connected into a ring bus. In this scenario, can a Generation Subsystem be one plant with multiple units each connected to a ring bus via individual generator step-up transformers? The meaning of "shared" needs to be defined. Generating Units may share elements in a ring bus in a substation, but the loss of one shared element may make only one generating unit unavailable and not the other generating units.
PacifiCorp	Disagree	See PacifiCorp's summary comments in question 13 and comments on BES Subsystem above in 1.c. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the "iron" (generating unit) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase "singularly or in combination." If the definition is needed, it should refer to the distributed control systems for BES generating units in scope.
PEPCO	Disagree	The current definition is confusing. The phrase -singularly or in combination-, brings significant uncertainty as to the intended objective. We suggest the following: BES Generation Subsystem - Generation plants or generation units including the BES Facilities required to connect them to a transmission system whose output could become unavailable due to loss or compromise of a BES Element or BES Cyber System.
NEI	Disagree	A) The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System". B) On November 16, 2009 NERC issued the "Final Report from the Ad Hoc Group for Generator Requirements at the Transmission Interface" defining what is considered part of 'generation' and what's part of 'transmission' in different interface scenarios. This definition does not embrace the granularity of that guidance. C) Clarification is sought on what exactly the phrase "including the Facilities required to connect them to a transmission system" entails. We believe this means transformers and transformer support systems, and want to ensure that this isn't construed as the generating station Control Room. D) Suggest the addition of "as defined by the local interface agreement" after "transmission system" to ensure the boundaries are clear to the Generator. E) Defining groups of generation facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it may vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the

Organization	Yes or No	Question 1.d. Comment (Response page 8)
		downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Summary Consideration: Summary Consideration: A number of respondents commented on the definition of Transmission Subsystem, citing vagueness and suggested the use of terms already defined in the glossary and in wide use in the industry. The SDT reviewed the comments and agreed that the use of terms already defined and widely used in the industry will serve the same purpose. The definitions for Subsystems have been removed and the references in the standard use terms already defined in the NERC Glossary or in wide use by the industry and any additional clarifying terms in the standard where "subsystems" were previously used.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
Progress Energy	Disagree	Remove "shared element or" from definition since these CIP standards are only intended to improve protections around cyber security assets.
GSOC/OPC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with "including transmission lines or busses" is unclear; if the intent is to say that "multiple transmission lines or busses whose combined output etc" must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term "output" with "capacity". The phrase "shared Cyber System" is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Hayden	Disagree	Need to emphasize connection to and support of the Bulk Electric System. Adding some sort of focus on the BES in this definition is needed.
SDGE		We are advocating a simpler approach to make the definition easier to understand and apply. We propose new wording as follows for clarification: Transmission substations, transmission busses, or transmission lines including the Facilities required to interconnect them.
APPA	Disagree	APPA Task Force Comments: See Comment for BES Subsystem. No comments on the SDT's proposed definition if this approach is adopted.
Consumers	Disagree	Although probably not the intent, this definition seems to limit the subsystem to only those assets "… whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System." In addition, it

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		should be noted that although a 'shared cyber system' may cause the loss of several BES elements, there may not be an impact to system reliability. See Section 13.
NPCC	Disagree	Definitions should not include impact Recommend the following definition - Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination.
MPPA	Agree	
Central Lincoln	Disagree	Again we fail to see how the part past the final comma adds any elements or clarity to the part that precedes it. And how does one determine whether the individual busses within a substation constitute individual subsystems, or whether the entire substation constitutes a subsystem? Although the guidance document states the level of granularity is up to the registered entity, the draft standard does not make this statement. As above, the definition should be modified to make it clear that transmission subsystems are a subset of the BES systems.
NERC	Disagree	1. The concept of "misuse" needs to be captured along side of the current concepts of availability, degradation and compromise; 2. The definitions and application of Transmission Subsystems and Generator Subsystems provides the opportunity for artificial behavior in categorizing impact levels. The categorization process could drive entities to de-couple cyber systems that support multiple assets within an existing subsystem in order to classify them as different subsystems, each with a corresponding lower impact level. Those actions can result in additional security weaknesses and possibly impact the reliable operations of the subsystem.
Dominion	Disagree	See comments to 1.b. and 1.d. above.
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	The definition needs to be tied back to the BES registration requirements similarly to the Definition for Generation Subsystems. This definition has the same duality problem as Generation Subsystems.
Dyonyx	Disagree	The use of the terms "Facility" and "Element" in the context of this CIP Reliability Standard in defining "Transmission Subsystem" is complicated by the convoluted nature of the definition of the former terms ("Facility" and "Element") in the current NERC Glossary of Terms and extends the confusion accordingly.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
FMPP	Agree	
Westar	Agree	
Green Country	Disagree	Does not draw a "bright line" around Generation switchyards as to the EXACT point it becomes transmissions responsibility.
Oregon PUC		The term “compromise of …” is too broad and leaves too much room for auditor and enforcement interpretation.
Manitoba 1	Agree	
Portland GE	Disagree	We propose “Transmission substations, transmission busses or transmission lines including the Facilities required to connect them to Elements, singularly or in combination.” Delete everything after “combination” in third line.
PSEG	Disagree	Comment #1: We believe that the proposed definition could be interpreted to two different ways. a. The definition is attempting to identify the Facilities in the substation (examples: Breakers, switches, tap changers and real-time data) controlled through a BES Cyber System. b. The definition is attempting to identify the BES Cyber System which controls the breakers, switches, tap changers and real-time data in a substation. The difference between the two interpretation is that one will contain a list of Facilities (Breakers, switches, tap changes) while the other contains a list of electronic devices control Facilities. It is our understanding that the first interpretation is the proper understanding and makes the following suggestion to the definition. Is made up of devices that are able to change state (open, close) change voltage levels (tap changers, cap banks) and collect real-time data (CT, VT, PMUs) and contained with a BES Cyber System. (NOTE: See our suggested definition of a BES Cyber System) Two Examples: 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. The goal of our suggested definition is to make it clear that a Transmission Subsystem can be made up of all, portion of or multiple substations based on an entities ESP configuration at the substation level. Comment #2: We believe that there is inconsistent use of terms compared to other NERC standards.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. We also support the revised

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		definition as proposed by EEI in their response to this revised standard.
Idaho Power	Disagree	Need to define element. It would be helpful to provide some examples of what might constitute a shared element.
SOCO	Agree	It should be noted that although the 'shared cyber system' may cause the loss of several BES elements, there may not be an impact to system reliability.
DTE	Agree	
AEP	Disagree	Defining groups of transmission facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.
Edison Mission	Disagree	The use of the terms "Facility" and "Element" in the context of this CIP Reliability Standard in defining "Transmission Subsystem" is complicated by the convoluted nature of the definition of the former terms ("Facility" and "Element") in the current NERC Glossary of Terms and extends the confusion accordingly.
Calpine	Agree	
NS&T	Disagree	See previous comment.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	Again, given the pervasiveness of SCADA/EM system connectivity, the definition establishes a nearly unlimited number of combinations, i.e. transmission subsystems.
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	What's an "Element" (one time capitalized, another not) – definition provides no clarity; counterproductive.
CenterPoint	Disagree	Disagree – See comments on 1.a, 1.c, 1.d, and 8. However, some of the concepts in this proposed definition could possibly be added to CIP-002-2 - R1.2.2 for additional clarification.
LCRA	Agree	
FRCC	Disagree	See comment to question 1.a.
NIPSCO	Disagree	We are concerned about the use of the word Subsystem within this definition as this does not appear within the NERC

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		glossary of terms. Suggestion: Clearly define the term subsystem within the NERC glossary and review the use of the terms facility and element within the proposed definitions.
ConEd	Disagree	Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
EEI	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective. We suggest: Transmission Subsystem — Transmission substations, protection systems, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared Element or shared BES Cyber System.
O&R	Disagree	Add “One or More” to beginning of definition to make clear that a Subsystem can consist of one facility or multiple facilities.
Alliant	Disagree	We believe the definition needs to be revised as noted below: "BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem." Please clarify the definition of "shared." The terms "transmission substation" and "transmission bus" need to be added to the NERC Glossary of Terms, and "transmission lines" should be replaced with "Transmission Lines."
Ameren	Disagree	The words "whose combined output" should be removed and replaced with "that". A transmission system does not output anything. The definitions of Generation Subsystem and Transmission Subsystem BOTH include "Facilities required to connect" generators to Transmission. Since FERC, RRO and virtually all state Commissions have the generator owning the GSU, ONLY the Generation Subsystem definition should only be included in "Facilities required to connect" generators to Transmission. What is the definition of “shared element”? This needs to be a defined term.
Black Hills	Disagree	Need to identify that this is a subset of the BES Subsystem definition. Might be better to stop the definition after the word 'combination'. What is the "combined output" of transmission lines? (Net MVA capability?). The last use of "element" should be "Element".

Organization	Yes or No	Question 1.e. Comment (Response page 9)
TNMP	Disagree	The phrase “whose combined output could become unavailable” is not clearly applicable to all Transmission Subsystems. A Transmission substation should always have a net of all inputs and outputs to be zero. None of the criteria in CIP-002 Attachment 1 look at the total output of a Transmission Subsystem to evaluate the Transmission Subsystem Impact rating. The definition should be rewritten to clear up any confusion.
NVEnergy	Disagree	With this definition, it is unclear what level of aggregation of the various busses, lines, stations, etc. is allowed or expected. The definition uses defined NERC terms as “Facilities” and “Elements”, yet the degree of granularity seems to be inconsistent (for example, how can a Transmission substation include Facilities that are required to connect with an Element). Note that much of the confusion in this definition is a result of our lack of understanding of the difference between the NERC-defined terms used here. Beyond that, however, the use of the phrase beginning with “including transmission lines…” infers that the definition is not limited to those collections of elements whose output could be subject to common mode loss, and therefore includes other collections of elements whose groupings are not well-defined.
MWDSC	Disagree	Appears to suffer from circular logic - by linking a substation to a cyber system, doesn't it force a conclusion that it has a medium or high impact?? Transmission Subsystems may become unavailable for many reasons, but loss of one substation or element may not affect an interconnected system. See following comments on impact levels.
Empire	Disagree	Alternative suggestion: A group of one or more transmission facilities operated at 200 kv and above that are controlled and monitored by a common BES Cyber System.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	A better definition of "Facilities" and what is included.
SCEG	Disagree	Strike "or shared Cyber System" per the comments in 1.d, or recommend changes to the language in R3.2. The definition is at odds with the proposed standard.
Exelon	Disagree	Exelon has concerns that the proposed definition may be open ended and subject to vastly differing interpretations (e.g. singularly or in combination) and suggest the following revisions: Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared BES Cyber System.
BPA Trans	Disagree	We propose “Transmission substations, transmission busses or transmission lines including the Facilities required to connect them to Elements, singularly or in combination.” Delete everything after “combination” in third line.
HQT	Disagree	Definitions should not include impact Recommend the following definition - Transmission substations, transmission busses, or transmission lines including the

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination.
Allegheny Supply	Agree	
KCPL	Disagree	No, this definition should limit itself to the transmission facility itself. The terms, “shared element or shared Cyber System” are too vague as to what that represents and, again, makes this definition conditional. The CIP standard should identify the facilities to be included for evaluation (as this is attempting to do) and allow the process for determining the impact a facility or facilities has on the BES to drive the appropriate level of cyber protection.
Connectiv Energy	Agree	Similar to the answer to 1d, one concern is that “Shared Element…” would be defined to include a Transmission Owner’s asset (farther up the line from a single plant connection) to which generating units from more than a single GO are attached? In this case would NERC look to aggregate generation from more than a single GO which singularly might not be part of the BES but due to their “Subsystem” connection could force them into the BES due to the combined total generation? This would not be desirable.
MidAmerican	Disagree	See MidAmerican’s summary comments in question 13 and comments on BES Subsystem above in 1.c. and 1.d. The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the “iron” (substation) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset. The CIP-002-4 definition, if needed, is confusing, especially the phrase “singularly or in combination” and in the use of NERC Glossary terms “Element” and “Facility.” As currently written, the definition’s scope could be a single circuit breaker up to and including all electrical facilities within a balancing authority area. Such a broad and vague term may cause difficulties implementing, auditing and proving compliance. If the definition is needed, MidAmerican proposes that its scope be limited to transmission substations and Special Protection Systems.
CPG	Disagree	This definition should clearly demarcate from the point of interconnection to the distribution system.
Santee Cooper	Agree	
OGE	Disagree	• Please provide a definition of "shared element" for electric transmission and other entities. • OG&E requests clarification on the “transmission subsystem” definition; Is there an expectation that every line segment be uniquely identified and classified? • OPTION: A group of one or more transmission Facilities controlled or monitored by a common BES Cyber System. Once clarity is achieved for what is meant by “common BES Cyber Systems”.
Oncor	Disagree	BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared Element or shared transmission Cyber System shall be considered as a single Transmission

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		Subsystem.
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Disagree	National Grid believes that the definition should not include impact and propose the following definition “Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination. Transmission substations, transmission busses, or transmission lines sharing an element or Cyber System must be additionally categorized in combination”.
MGE	Disagree	Since the term BES is defined by NERC as usually 100kV and above, then this definition only applies to a Transmission Subsystem(s) connected at 100kV or greater. Refer to question 1.a. concerning a shared “Cyber System”. As written if there is no “shared element” then the stand alone Transmission Subsystem connected at 100kV and above is not a Transmission Subsystem. Please clarify what a “shared element” refers to. Is this a cyber element that is common to two generators or could this be a non cyber physical element? Recommend that physical elements (non cyber) not be covered by CIP Standards.
FE	Disagree	The term "shared element" is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared "Cyber System" to shared "BES Cyber System".
TECO	Disagree	We support EEI’s comments and suggest the following changes to the definition. Transmission Subsystem — Bulk Electric System Transmission substations, protection systems, transmission busses, or transmission lines including the Facilities required to connect them to Elements, including transmission lines or busses whose combined output could become unavailable due to loss, compromise, or significant degradation of a shared BES Cyber System.
CECD	Disagree	The definition should be modified as follows: Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System.
MRO	Disagree	We feel the definition is ambiguous as written, and would propose the following reworded definition for clarity: BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem. We also would like a clarification of “shared” as we had disagreement just within our MRO NSRS group on what this term

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		implied. Regardless, the terms “transmission substation” and “transmission bus” should be defined in the NERC Glossary of Terms, and “transmission lines” should be replaced with “Transmission Lines” to remove further ambiguity.
GTC	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including transmission lines or busses” is unclear; if the intent is to say that “multiple transmission lines or busses whose combined output etc” must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term “output” with “capacity”. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
Xcel	Disagree	We feel the definition is ambiguous as written, and would propose the following reworded definition for clarity: BES transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements. Transmission lines or busses whose combined flows could become unavailable due to loss or compromise of a shared transmission Element or shared transmission Cyber System shall be considered as a single Transmission Subsystem. We also would like a clarification of the term “shared”. The terms “transmission substation” and “transmission bus” should be defined in the NERC Glossary of Terms, and “transmission lines” should be replaced with “Transmission Lines” to remove further ambiguity
BGE	Disagree	Change “Cyber System” to “BES Cyber System” The term, “shared element” is vague and may include items unrelated to cyber security. We recommend that the term “shared element” be omitted. We recommend the following definition. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared BES Cyber System. Communication networks and data communication links between discrete BES cyber systems need not be considered as a “shared cyber systems” in the determination of facilities that constitute BES Subsystem. Even with this modification, we are concerned that the definition is overbroad in that there is no limit to combining disparate systems and considering them a single subsystem.

Organization	Yes or No	Question 1.e. Comment (Response page 9)
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Agree	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	The current definition is confusing. The phrase “singularly or in combination,” brings significant uncertainty as to the intended objective.
FMPA	Disagree	See FMPA’s comments to 1.d.
Duke	Disagree	This definition should be revised to remove ambiguity. Suggested wording: Transmission Subsystem – Transmission substations or Transmission lines.
NBSO	Disagree	Recommend including wording to ensure that that the definitions are only used for the determination of critical cyber assets. The concern is that these definitions may be used inappropriately in the development/revision of non-cyber related standards.
AESI	Disagree	If "element" in the Generation and Transmission Subsystems definitions means what it does in the Glossary, it should be capitalized. If not, what does it mean? The intent of the phrase beginning with “including transmission lines or busses” is unclear; if the intent is to say that “multiple transmission lines or busses whose combined output etc” must be treated as a single Transmission Subsystem, this should be clarified; if this is not the intent, it is difficult to see what the phrase adds to the definition. Also, in this case we suggest you replace the term “output” with “capacity”. The phrase “shared Cyber System” is vague – what constitutes a shared Cyber System? A device used by multiple BES Subsystems? Devices on a shared network? Devices in a shared physical perimeter? Devices administered by the same staff? Any of these situations could mean that if one Subsystem is impacted, there is potential for impact to other Subsystems, but it is unclear which of these situations need to be considered.
IESO	Agree	
Manitoba 2	Disagree	Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	ATC believes that the proposed definition could be interpreted in two different ways. 1. The definition is attempting to identify the Elements in the substation (examples: Breakers, switches, tap changers and real-time data) controlled through a BES Cyber System. 2. The definition is attempting to identify the BES Cyber System which controls the breakers, switches, tap changers and real-time data in a substation.

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.e. Comment (Response page 9)</th></tr>
<tr><td></td><td></td><td>The difference between the two interpretations is that one will contain a list of Elements (Breakers, switches, tap changes) while the other contains a list of electronic devices that control Elements.

It is our understanding that the first interpretation is the proper understanding and we make the following suggestion:

“Is made up of devices that are able to change state (open, close) change voltage levels (tap changers, cap banks) or collect real-time data (CT, VT, PMUs) and contained within a BES Cyber System.”

(NOTE: See our suggested definition of a BES Cyber System)

Two Examples:

1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystems.
2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem.

The goal of our definition is to make it clear that a Transmission Subsystem can be made up of all, portion of or multiple substations based on an entities ESP configuration of its BES Cyber System.</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network</th><th>Physical</th><th>Data</th><th>Antivirus</th><th>OS</th><th>Intrusion</th><th>Account</th><th>Firewall</th></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.e. Comment (Response page 9)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Connections</th><th>Perimeter</th><th>Encryption</th><th></th><th>Patches</th><th>Detection</th><th>Passwords</th><th></th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Puget Sound Energy requests clarity of the term Transmission.

Transmission Subsystem- Bulk Electric Transmission Facilities including substations, protection systems, transmission busses, or transmission lines and equipment required to connect them to Elements, that could become unavailable due to loss or compromise of a shared BES Cyber System.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The definition is not clear and very confusing. IMPA recommends clarifying what exactly is meant by the terms “singularly or in combination” in the definition of the Transmission Subsystem. In addition, it would help with the clarity of the definition if transmission busses and transmission substation were defined in the NERC glossary. The term transmission lines should be changed to reference the NERC glossary (Transmission Lines).

The meaning of “shared” needs to be defined.</td></tr>
<tr><td>PacifiCorp</td><td>Disagree</td><td>See PacifiCorp’s summary comments in question 13 and comments on BES Subsystem above in 1.c. and 1.d.

The definition is not needed at this time and not until it is proven that security controls categorization of high, medium or low correlate to the size of the “iron” (substation) the Cyber Asset supports as opposed to the characteristics of the connectivity and/or span of control of the Cyber Asset.

The CIP-002-4 definition, if needed, is confusing, especially the phrase “singularly or in combination.” The definition as currently written should specify more clearly the scope of the term. As currently written, the definition could be a single</td></tr>
</table>

Organization	Yes or No	Question 1.e. Comment (Response page 9)
		circuit breaker to all electrical facilities within a balancing authority area. Such a broad and vague term may cause difficulty for auditing as well as for proving compliance. If the definition is needed, PacifiCorp proposes that is scope be limited to transmission substations, protection systems, transmission busses or transmission lines.
PEPCO	Disagree	The current definition is confusing. The phrase - singularly or in combination - brings significant uncertainty as to the intended objective. In addition while the transmission subsystem consists of the various elements described in addition to other elements such as transformers, we believe that the cyber security standards if using the Big Iron method should classify at the substation level (i.e. the bus(es), line(s), or transformer(s) help determine the impact level of the substation). The phrase - including transmission lines or buses whose combined output could become unavailable - is confusing as transmission subsystems usually are not referred to as having output like generators. Rather than output, transmission subsystems have throughput or capability/capacity. We suggest the following: BES Transmission Subsystem — BES Transmission substations made up of BES Elements and BES Facilities (e.g. BES transmission busses, BES transmission lines, and/or BES transformers) which could become unavailable due to the loss or compromise of a BES Element or BES Cyber System.
NEI	Disagree	A) Revise to “Transmission substations and transmission lines.” B) If A) is not followed, the term “shared element” is not needed in this definition. It implies a need for physical protection of a common mode non-Cyber System device/element. This standard, and the proposed definition, should focus on guarding against compromise of a shared Cyber System. We also recommend changing shared “Cyber System” to shared “BES Cyber System”. C) Defining groups of transmission facilities on the basis that the facilities share a common cyber security system suggests a common risk level that does not exist. Each facility and the cyber security systems contained within it mat vary significant with regard to the likely threats, vulnerabilities, and BES impacts. While the concept of grouping seems to provide for simplicity in assessing the potential adverse impacts to the BES, this simplicity has the downside of not differentiating where the true risks are to the BES. Again, this may have the unintended consequence of spreading security resources so far that the truly critical devices and systems with the greatest potential for adversely impacting the BES is actually diminished rather than enhanced.

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

Summary Consideration: Many respondents commented that the definition of Control Center needed more specific bounds. The SDT has modified the definition to add more specificity. The new definition is shown below, with the changed words highlighted in yellow:

A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
Progress Energy	Disagree	The definition of Control Center needs to specify that control rooms in power plants or transmission substations are NOT included in the definition of Control Centers.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
Dynegy	Disagree	1. The term “BES assets” is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: “A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…” 2. In the third bullet, the terms “and asset management” need to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term “BPS” should be replaced by “BES”.
GSOC/OPC	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity. With respect to the first bullet of the definition, we suggest changing it to the following ”Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control systems; or automatic load-shedding systems” We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a control center. The phrase “capable of” is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term “Situational awareness”.
Hayden	Agree	
SDGE	Disagree	For clarification, we propose new wording for this definition as follows: A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations performed by a Control Center include, but are not limited to, one or more of the following: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems • Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		information used by Responsible Entities to make operational decisions regarding reliability and operability of the BES) • Coordination of BES restoration activities.
APPA	Disagree	APPA Task Force Comments: Control Center The definition of Control Center needs clarification. There are primary and back-up Control Centers that have the assigned and contractual responsibility for the functions listed in the Control Center definition described in Version 4 that are performed by a Balancing Authority and Transmission Operator with Reliability Coordinator oversight. There are owners of distribution facilities who also own BES assets who have alarm monitoring and data collection capabilities for these facilities and assets but they do not and will not have remote supervisory control for BES assets. The facilities and BES assets of these owners who are merely monitoring and collecting information should not be required to have their facilities classified as Control Centers under the CIP standards. These owners have contracted with other entities to perform Control Center functions. A change to this proposed definition is needed to ensure that that an owner's identification of alarm monitoring capability does not make the facility subject to the Control Center requirements. For this reason, the fourth bullet under the Control Center definition, "Alarm monitoring and processing" should be changed to "Alarm processing".
Consumers	Disagree	Why the use of the term, Bulk Power System? Also, an equipment room containing a front-end processing unit which received data from multiple substations would perform the function listed in the second bullet and therefore qualify as a control center. At power plants, often the unit control room controls the generating unit (or multiple units) and also has supervisory reclosing capability of the generator high side breakers out in the plant switchyard. Therefore, this control room may be pulled into scope unintentionally. Also, we are reintroducing the term assets, without definition.
NPCC	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
MPPA	Agree	
Central Lincoln	Disagree	This definition might be interpreted to encompass every laptop computer or PDA outfitted with SCADA web client and/or alarm processing software. Suggest language that would clarify that fixed server locations are intended, and that remote clients are not. The term "BES asset" should also be defined. The first bullet implies all load-shedding systems, for example, are BES assets. The definition should be narrowed so that only those load-shedding systems that have a BES reliability impact are included. Perhaps "BES facility" should be used instead, in order to be consistent with the other proposed definitions.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
NERC	Agree	
Dominion	Disagree	Dominion disagrees with the definition of “Control Center.” Under the current definition, any one attribute, such as displaying system status or having a space dedicated to coordination of restoration, could qualify as a “Control Center.” The definition is too broad and should be modified to emphasize that a “Control Center” should have the capability for: 1) data display; and 2) system control. Also, the listed examples should be illustrative as areas of consideration but not as specific qualifiers.
Encari	Disagree	“Control Center” is said to be capable of performing one or more of the functions for multiple (i.e., two or more) BES assets. The emphasis on “capable” invites confusion. A SCADA system may actually be used to control a single substation but be capable of controlling two substations if the SCADA system had the appropriate supporting network communication and configuration settings. The criteria for a control center should focus on its actual configuration and use, not its theoretical capability. The term “BES asset” is neither defined in the NERC Glossary nor in the Standard. For purposes of consistency, the term “BES Subsystem” should replace the term “BES asset” since both terms appear to have the same meaning within the Standard. “BES Subsystem” is preferred since it is explicitly defined in the Standard. Additionally this definition of control center may lead to confusion due to the generic interpretation of "alarm monitoring and processing". Specifically this may include fire alarm systems, water suppression systems, physical security operation centers and any other centralized function with "alarm monitoring and processing". We recommend strengthening this definition to be more specific.
US ACE – NW	Disagree	Control center definition should not apply to multiple facilities that are located on the same property where data/controls are aggregated to a central control room. For example wind generators each have data collection and control systems in each tower and that data is fed to a central control room that is physically on the same property and commonly contained within the same physical security boundaries. Another example would be the many thermal and hydropower generating facilities that have multiple powerhouses on the same physical property with all controls centralized. So, the Control Center definition needs to only apply to those generating or transmission facilities that are not all located on the same physical property.
SCE	Agree	
USBR	Disagree	The definition implies a definition for BES assets which is not covered in the NERC Glossary. It should either define BES Assets or be modified to refer to BES Subsystems. As such the text following BES assets should be deleted. The third bullet item is redundant to the second bullet and should be deleted. The forth bullet is covered under the second bullet and should be deleted.
Dyonyx	Disagree	The definition of “Control Center” uses new terms that have not previously been defined which will add to the confusion in understanding the definition. Specifically, the term “BES Assets” is not defined. Why not use the term “BES Subsystem”

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		or the proposed “BES Facility”? In terms of categorizing the “Impact” of a Control Center “Subsystem”, we believe it is important to realize that the “Impact” categorization of a Control Center is dependent upon the “Impact” of the underlying “Cyber Systems” contained within the Control Center. Accordingly, not all Control Centers are High Impact or even Medium Impact Subsystems. An iterative process will be required to properly establish the categorization of this particular BES Subsystem.
FMPP	Agree	
MISO	Disagree	The following changes need to be made to this definition: 1. The term “BES assets” is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: “A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…” 2. In the third bullet, the terms “and asset management” need to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term “BPS” should be replaced by “BES”.
Westar	Disagree	Bullet one includes 'automatic load-shedding systems'. Underfrequency Load Shed programs, which I think would qualify as an automatic load-shedding system, are typically installed on the distribution system and not on the BES. Will this pull the pure Distribution Control Centers into the CIP requirements? Suggest eliminating the 'or automatic load-shedding systems'.
Green Country	Disagree	How does this affect previous definitions of "Control Room" and "Control Center". With respect to generation I believe the "Control Room" definition is appropriate. Control Room - A Control Room is typically located within the facility and operates control systems limited to controlling: 1. A single generation plant with one or more units. 2. A single transmission asset such as a transmission substation.
Oregon PUC		No comment
Manitoba 1	Agree	
Portland GE	Disagree	This definition has the potential for making substation control houses, or other facilities, where some type of control is exerted over more than one substation facility, fit within the definition of a “control center.” The NERC definition of Control Center should be consistent with what the Utility Industry normally uses to identify "Control Centers". We suggest a more concise definition as follows:

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		Control Center – "A Facility from which System Operators (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) monitor and control transmission or generation Facilities in real time." The definitions of these terms from NERC Glossary of Terms Used in Reliability Standards, updated April 20, 2009 were considered and used to develop the recommended definition: System Operator, Transmission Operator, Transmission, Generator Operator, Telemetering, Facility, and Element.
PSEG	Disagree	Comment #1: We mostly agree with the proposed definitions however, we question if NERC RCIS, NERC TLR; MISO Outage Scheduler, MISO Information System, OATI – would then fit this definition of a Control Center unintentionally. Comment #2: We would like to understand the intention of the substitution of the terms Bulk Power System (BPS) for Bulk Electric System (BES) in this definition.
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI's comments regarding this definition. We also support the revised definition as proposed by EEI in their response to this revised standard.
Idaho Power	Agree	
SOCO	Disagree	While a specific definition of what constitutes a control center is necessary, a literal reading of the definition given would include far more facilities than are intended. For example, an equipment room containing a front-end processing unit which received data from multiple substations would perform the function listed in the second bullet and therefore qualify as a control center. While a good faith reading of the standard would not produce such results, good faith cannot be relied upon in all cases, so the definition must be tightened At power plants, often the unit control room controls the generating unit (or multiple units) and also has supervisory reclosing capability of the generator high side breakers out in the plant switchyard. Therefore, this control room may be pulled into scope unintentionally. The term "assets" should be identified – is this intended to mean "BES subsystem"? Suggested definition: A Control Center is capable of performing one or more of the functions listed below for geographically dispersed multiple sites (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: … This definition should be worded to delineate that it is not intended to included independently isolated generation units controlled from within the same control room or building. A control room for a two unit generation plant could interpreted to be included under the second bulleted item. Suggested insertion at bottom of definition: This is not intended to include control rooms at power plants intended exclusively for the control of generation units.
DTE	Agree	

Organization	Yes or No	Question 1.f. Comment (Response page 10)
AEP	Disagree	The open-ended nature and lack of clarity in this definition is concerning for the reasons described in the response to question 1a. This generally results from the approach of incorporating many technical functions into a single definition. As a result, there is a lack of clarity as to what is intended to be in scope and out of scope. For example, the descriptions could, perhaps unintentionally, even draw in plant control rooms or unit control rooms.
Edison Mission	Disagree	The definition of "Control Center" uses new terms that have not previously been defined which will add to the confusion in understanding the definition. Specifically, the term "BES Assets" is not defined. Why not use the term "BES Subsystem" or the proposed "BES Facility"? In terms of categorizing the "Impact" of a Control Center "Subsystem", we believe it is important to realize that the "Impact" categorization of a Control Center is dependent upon the "Impact" of the underlying "Cyber Systems" contained within the Control Center. Accordingly, not all Control Centers are High Impact or even Medium Impact Subsystems. An iterative process will be required to properly establish the categorization of this particular BES Subsystem.
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	Existing definition of control center is sufficient. Currently control center does not include a dispatch center at a local distribution entity that may or may not be staffed 24-hours and does not function as a BA, TO, GO, or RC. The definition of control center should not be expanded with this standard. See current NERC Glossary re definition of a System Operator. System Operator An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.
E ON	Disagree	Bullet two would establish as a control center any location where BES reliability or operational data is being displayed. The same bullet would also qualify a Remote Transmitting Unit ("RTU") as a Control Center. The third and fourth bullet would establish nearly every substation control house, and any other facility housing control panels with alarm indicators and acknowledgement capability, as Control Centers. Clearly, the definition is far too encompassing. The drafting team would be well advised to pay particular attention to use of the conjunctives "and" and "or" in this standard.
Carthage		Again CWEP would like better clarification on BES. Please refer to 1C above.
WECC	Agree	Is the intent of this definition to bring in new entities that haven't previously been identified as having impact on the BES such as Market Control Systems?
Entergy	Disagree	This is not a definition – it's a list of examples of what might be that which is ill-defined.
CenterPoint	Disagree	Disagree – See comments on 1.a. However, some of the concepts in this proposed definition could possibly be added to CIP-002- 2 - R1.2.1 for additional clarification.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
LCRA	Disagree	1. More explanation and definition is required as to why asset management is included. Asset management functions would normally not be essential for the operation and control of the BES Subsystem. Need to better define what specific asset management functions are included. 2. "BPS" is not defined. What does this mean?
NIPSCO	Disagree	We mostly agree with the proposed definition however, we question if the definition unintentionally expands the scope to include cyber systems that support real-time operations within the control center environment: RCIS, TLR, ARS, RC Outage Scheduler, RC Information System, OATI, etc.. Additionally, we would like to understand if it was the intention of the SDT to substitute the terms Bulk Power System (BPS) for Bulk Electric System (BES) in this definition only. Suggestion: Review the intended scope of the term control center and clarify the intent with revised or additional language.
ConEd	Agree	
EEI	Disagree	Parts of the definition are too broad. For example, a literal interpretation of: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations" Could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. We suggest: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential used for real-time operations" • Bullet 4, "Alarm monitoring and processing", should be changed to read "BES alarm monitoring, processing and response.."
O&R	Agree	
Alliant	Disagree	We believe the bullet "Alarm monitoring and processing" should be removed, as this functionality should inherently be included as part of the other processes listed. In some instances, it is even directly redundant as written.
Ameren	Disagree	Change "BPS" to "BES" to be consistent with the rest of the document. The definition of Control Center has expanded significantly. We believe that the definition needs to focus more on the control aspects and not simply on the display of data. In the third bullet, the term "and asset management" needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. The Control Center should only include those facilities where NERC certified operators are required for its operation.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
Black Hills	Agree	
TNMP	Agree	TNMP agrees with the proposed definition. The inclusion of multiple BES assets in the definition is important to help draw a distinction between Control Centers and substation HMIs.
NVEnergy	Agree	
MWDSC	Disagree	Alarm monitoring and processing, as well as coordination of restoration activities, is a real time function involving action by a Transmission or Generator Operator. Other entities may have redundant alarms at a facility, but will be contacted by the Transmission Operator as necessary to coordinate activities. Recommend adding a phrase to the definition such as ""A Control Center of a Transmission Operator or Generator Operator which is capable of performing ….."
Empire	Disagree	Optional definition: BES Control Center-A facility used to perform the function of an RC, BA, TOP, GOP or LSE in the real time operation of the BES.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	The problem again is what is the BES.
SCEG	Disagree	There is an opportunity for confusion between a "control room" at a power plant and a "control center", which only applies if two or more BES assets are being controlled. It would be better to use a more descriptive term such as "centralized control center" to more clearly indicate the distinction.
Exelon	Disagree	Exelon is concerned that the proposed definition may be interpreted by some to include dedicated generation plant control rooms (with more than one generator), as a result we recommend an exclusion statement be added to add clarification. We suggest the following be added: A control room shall not be categorized as a Control Center. A control room is typically located within the facility and operates control systems limited to controlling: A single generation plant with one or more generation units, A single transmission asset such as a transmission substation
BPA Trans	Disagree	This definition has the potential for making substation control houses or other facilities, where some type of control is exerted over more than one substation facility, be defined as a “control center.” Our definition for Control Center is: “The facility from which a power system is monitored and regulated. Dispatchers use computerized displays to match generation with load and to respond to faults in the system.” The NERC definition of Control Center should be consistent with what the Utility Industry normally uses to identify

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		"Control Centers". We Suggest a more concise definition as follows: Control Center – "A Facility from which System Operators (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) monitor and control transmission or generation Facilities in real time." The definitions of these terms from NERC Glossary of Terms Used in Reliability Standards, updated April 20, 2009 were considered and used to develop the recommended definition: System Operator Transmission Operator Transmission Generator Operator Telemetering Facility Element
HQT	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
CCG	Disagree	The definition of Control Center as described is overly broad. Specifically, the second bullet unintentionally includes tagging systems or any display of generation management system data that does not have the ability to directly affect real-time operations. In addition, the words "asset management" should be removed from bullet three. Asset management is an overly broad term that could be unintentionally applied to generation management systems without the ability to directly affect real-time operations.
Allegheny Supply	Agree	
KCPL	Disagree	Disagree with the third bulleted item. Asset management has nothing to do with the maintaining the reliability of the BES. Recommend modifying the third bulleted item to, "System status monitoring and processing for reliability purposes".
Connectiv Energy	Disagree	This can be agreeable if the wording "multiple (i.e., two or more) BES assets) such as generating plants…" is not later interpreted to mean two or more BES Assets such as generating UNITS at a single plant.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
MidAmerican	Disagree	This definition is not needed for two reasons. First, the existing non-CIP NERC standards have requirements for transmission control centers. Transmission control centers subject to those non-CIP NERC standards should be in scope. Second, if a generating unit is in CIP scope, then the Cyber Assets for the distributed control system for the generating unit should be evaluated to determine if they meet the criteria to be in CIP scope. Definition of a generation control center is not needed. The CIP standards must harmonize with and maintain the integrity of the other NERC standards. The proposed definition is problematic because it diverges from and possibly contradicts the other standards. If this definition were adopted in the Glossary, would the additional control centers it defines be subject to the other NERC standards for transmission control centers? If a definition is needed, it needs to be bright line, in contrast to the vague proposed definition. It must incorporate concepts of the other NERC standards for transmission control centers.
CPG	Disagree	The functions of a Control Center are too broad and will impact unintended operations centers, which do not have an effect on the BES.
Santee Cooper	Disagree	Need some clarification concerning distribution control centers. SC does not want to classify it as a Control Center as it pertains to theses standards. It would cause unnecessary additional work and studies.
OGE	Disagree	OPTION: BES Control Center – a facility used to perform the function of an RC, BA, TOP, GOP or LSE in the real time operation of the BES.
Oncor	Disagree	Restated - A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES Facilities. Change BPS to BES in bullet 3
PPL Supply	Disagree	Comments: We mostly agree with EEI comments but would offer one additional clarification by adding the word "reliability" in EEI's proposed definition as per below: Parts of the definition are too broad. For example, a literal interpretation of: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations" Could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. We suggest: • "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time RELIABILITY operations"
St. George	Agree	

Organization	Yes or No	Question 1.f. Comment (Response page 10)
NGRID	Disagree	• Please explain BES Reliability Data • The whitepaper distinguished Control Rooms and Control Centers by number of geographic locations they control. • National Grid recommends changing the first bullet to "Supervisory control of geographically separated BES Subsystems" (see white paper) Also, change "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations." to "A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location."
MGE	Disagree	The qualifier of BES is in the definition of Control Center. But is missing in the forth bullet "Alarm monitoring and processing". Recommend that the forth bullet be completely removed, it allows for interpretation by regulators and does not fit with the overall approach of the other BES level functions, it is a sub-set of SCADA.
FE	Disagree	1. The term "BES assets" is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: "A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations..." 2. For consistency, we recommend using BES, not BPS (see third bullet).
TECO	Disagree	We support EEI's Comments and wording changes. In addition we suggest: The term "BES Assets" in the definition of Control Center should be changed to "BES Subsystems."
CECD	Disagree	The references to generation plants and transmission substations should be replaced with the terms being defined, i.e. BES Generation Subsystem and BES Transmission Subsystem. The functions of a Control Center described are too broad and will unintentionally pull in operations centers that should be left out of the definition because they have little or no impact on the BES. This broad application goes against the purpose of the standard, which is to apply security controls commensurate with the potential impact to the reliability of the BES. One of the defining lines for determining if an entity is a BES user, owner or operator is whether the equipment is operated at 100 kV or above. A generation subsystem or transmission subsystem has a one line diagrams by which the connectivity can be evaluated. A control center is more appropriately considered a Cyber System to be evaluated in relation to BES Generation or BES Transmission Subsystems. CECD supports a definition of BES Subsystem that allow for flexibility by the registered entity to define their BES Subsystem, including the ability to exclude a control center as a BES Subsystem

Organization	Yes or No	Question 1.f. Comment (Response page 10)
MRO	Disagree	We feel the bullet “alarm monitoring and processing” should be removed, as this functionality should inherently be included as part of the other processes listed. In some instances, it is even directly redundant as written. We also feel the terms “generation plants” and “transmission substations” should be defined in the NERC Glossary of Terms, and “transmission facilities” should be replaced with “Transmission Facilities” to remove ambiguity.
GTC	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity. With respect to the first bullet of the definition, we suggest changing it to the following ”Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control systems; or automatic load-shedding systems” We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a control center. The phrase “capable of” is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term “Situational awareness”.
BGE	Disagree	Why is the term BPS used as opposed to BES? What is the definition of BPS as it is used here?
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	For the first bullet, consider striking reference to Automatic Generation Control (AGC) systems as this may cause confusion in ISO/RTOs where the scheduling agent may not be the operational organization responsible for the Generator Subsystem. Also, there are many cases where AGC controls only a small subset of the total MWs and may be used for sending market signals rather than for reliability. This definition as written would classify power marketers as Control Centers when they have no ability to access controls. Regarding the fifth bullet , consider striking entire line. Alarm monitoring and processing is not a control function. There may be operational groups within an organization that receive read-only alarms, but that may not have access to control system functions. Receiving an alarm or having the ability to monitor should not in and of itself make this a Control Center.
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	Parts of the definition are too broad. For example, a literal interpretation of: “Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations” could lead a party to believe that any display of any BES reliability or operability data creates a

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		Control Center. An alternate definition suggestion is: “Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time operations”
FMPA	Disagree	See FMPA’s comments to 1.d. Use NERC Glossary defined terms: “BES assets” should probably become “Facilities”; “facilities” should become “Facilities” What does the “and system” refer to in the third bullet, “BES and system” since the BES is a system (Bulk Electric System)? Typo in this same third bullet, “BES” instead of “BPS”
Duke	Disagree	This definition should be revised to clarify that the definition of Control Center does not include the control room for a multiple unit site (which would be included as part of the Generation Subsystem). Need to delete the 4th and 5th bullets because “alarm monitoring and processing” and “coordination of BES restoration activities” are not associated with functional control. Suggested wording: Control Center - A Facility for control of multiple (i.e. two or more) BES Subsystems. Functions that support real-time operations of a Control Center typically include one or more of the following: • Supervisory control of BES Subsystems, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems. • Acquisition, aggregation, processing, inter-utility exchange, or display of BES data required for BES reliability or operability. • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
NBSO	Disagree	The Critical Asset Identification Guideline distinguished Control Rooms and Control Centers by how many geographic locations were controlled. Recommend changing “A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations.” to “A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations, at more than one location.”
AESI	Disagree	The first sentence says the functions listed below are what a Control Center performs. If the definition is intended to be more open-ended and these only illustrative, the first sentence should omit "of the" before "functions" and add the phrase "such as those" before "listed below": "one or more functions such as those listed below...." The second sentence should also be removed for clarity.

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		With respect to the first bullet of the definition, we suggest changing it to the following ”Supervisory control (manual or automated) of Facilities, including generation plants, transmission facilities, substations; Automatic Generation Control systems; or automatic load-shedding systems” We disagree with the second bullet of the Control Center definition. There are many systems that provide for acquisition, aggregation, processing, inter-utility exchange, or display of data for multiple Facilities. These systems do not constitute a control center. The phrase “capable of” is too vague and over-reaching; many systems may be capable of performing a given task, however they may not be performing it currently and the effort required to configure them to do so could vary significantly. This bullet should be removed or otherwise made consistent with an item on Attachment 2. With respect to the third and fourth bullets we suggest replacing them with the single term “Situational awareness”.
IESO	Disagree	Third bullet should read "operability of the BES" not BPS. The fourth bullet regarding alarm monitoring should be more specific to the types of alarms monitoring and processing.
Manitoba 2	Disagree	This definition should refer to BES Subsystems, not BES assets, as currently written. Control Centres for small generation resources, below the NERC registration threshold (20 MVA), should be excluded from this definition, up to a defined total output aggregate. The Reliability Coordinator and Balancing Authority functions may need to be explicitly included in Attachment 2. Alarm monitoring and processing should be specific to operation and restoration functions of the Control Centre. The term “BPS” in the third bullet needs to be changed to “BES”. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA	Disagree	Alarm monitoring and data collection capabilities that do not and will not have remote supervisory control for BES assets should not be included in this definition. Many owners of facilities and BES assets monitor and collect information via SCADA; however, do not allow control of facilities and BES assets via SCADA. These owners should not be included in this Control Center definition. This separate line item should be removed from this definition.
ATC	Agree	
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.f. Comment (Response page 10)</th></tr>
<tr><td></td><td></td><td>efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>The definition of the Control Center should not be confused with identifying the tools used to perform critical functions. For example the mention of display of BES reliability or operation data does not make a control center as this data may be displayed as read only even in real time. In general the second bullet should be deleted from this definition.</td></tr>
</table>

Organization	Yes or No	Question 1.f. Comment (Response page 10)
IMPA	Disagree	IMPA feels that the bullet "alarm monitoring and processing" should be removed. The term "processing" is ambiguous. IMPA recommends the following changes to the definition: Control Center - — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as Generation Subsystems or Transmission Subsystems. Functions that support real-time operations of a Control Center typically include one or more of the following: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems • Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations • BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS) • Coordination of BES restoration activities.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. Should further address the nuances regarding Control Centers that are not affiliated with specific generation plants or transmission substations. This would be appropriate for addressing the Control Center functioning as an RC, BA, or TOP. Midwest ISO Comments: The following changes need to be made to this definition: 1. The term "BES assets" is too vague and needs to be clarified. For example, if a BES asset was interpreted to mean a generating unit rather than a generation plant then the Plant Control Room for a multi-unit plant would fit this definition of Control Center. Suggest modifying this definition to read as follows: "A Control Center is capable of remotely performing one or more of the functions below for multiple (i.e. two or more) BES assets, which include generation plants (not individual generating units) and transmission substations…" 2. In the third bullet, the terms "and asset management" need to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition. 3. In the third bullet the term "BPS" should be replaced by "BES".
PacifiCorp	Disagree	This definition is not needed for two reasons. The term "control center," though not defined in the NERC Glossary of Terms, is already used in the context of other NERC reliability standards. For example, as defined in the NERC Glossary, a System Operator is an "an individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time. These control centers referenced in other NERC reliability standards should be the same as those defined by CIP standards. As currently drafted, the definition of Control Center will be different for CIP than for other NERC reliability standards. If it is needed, the current definition modified to remove the ambiguous language contained in the second bullet. Taken literally, this definition could include any BES reliability or operability display. PacifiCorp suggested modifying the definition to

Organization	Yes or No	Question 1.f. Comment (Response page 10)
		read: "Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data essential for real-time operations."
PEPCO	Disagree	Parts of the Control Center definition are too broad. For example, a literal interpretation of - Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations - could lead a party to believe that any display of any BES reliability or operability data creates a Control Center. Another example, a literal interpretation of - automatic load-shedding systems - could mean that a UFLS relay or a UVLS relay is a Control Center. We suggest the following: BES Control Center — A Control Center is capable of performing one or more of the functions listed below for two or more BES Generation Subsystems and/or BES Transmission Subsystem. Control Center functions that are used for real-time operations of the BES typically include one or more of the following: Bullet 1, Supervisory control of BES assets, including BES Generation Subsystems or BES Transmission Subsystem. Bullet 2, Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data used for real-time operations. Bullet 3, BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing BES information used by Responsible Entities to make operational decisions regarding reliability and operability of the BES). Bullet 4, Alarm monitoring and processing, should be changed to read BES alarm monitoring and processing.
NEI	Disagree	A) Clarify that the "Control Center" is not the control room of a multi-unit site (include in definition). It is expected that this "Control Center" is part of the transmission system. B) Delete the last two bullets. C) On third bullet, change BPS to BES. D) The open-ended nature and lack of clarity in this definition is concerning for the reasons described in the response to question 1a. This generally results from the approach of incorporating many technical functions into a single definition. As a result, there is a lack of clarity as to what is intended to be in scope and out of scope. For example, the descriptions could, perhaps unintentionally, even draw in plant control rooms or unit control rooms.

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures. or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures; or
- could hinder restoration to a normal condition.

Summary Consideration: There were many comments on the need for definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1. The SDT reviewed them and has removed these definitions.

Many also commented on the absence of a "No Impact" category. It is the SDT's opinion that the definition of BES Cyber Systems effectively removes Cyber Systems with no impact from the scope, and that a BES Cyber System has some level of impact, by definition.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
Progress Energy	Disagree	In 1st bullet, change to: "they could directly & immediately cause" For sub-bullets under 1st bullet add: "unacceptable risk to IROL" and remove or better define "BES separation; and/or a cascading sequence of failures." Remove 2nd and 3rd bullets since the planning time frame and restoration doesn't impact real-time operational reliability. More generally, the scope of CIP standards should only address real-time cyber operations.
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The second bullet of the definition is largely redundant to the first bullet and improperly references "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		"restoration" will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion. Should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to "restoration" will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
GSOC/OPC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized? The use of the phrase "unacceptable risk" makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase "could … cause" is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase "could hinder" is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Hayden	Agree	

SDGE	Disagree	We propose changing the wording as follows for clarification: BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:
		
		• they could directly cause, contribute to, or create
		  – BES instability; and/or
		  – BES separation; and/or

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		– a cascading sequence of failures. If a "risk statement" is included in this definition, the ability to quantify the risk is required, e.g., significance of the risk and probability of the risk. Additionally, if a risk statement is made in the "High BES impact" case, then there should be a similar risk statement in the "Medium BES impact" case with objective criteria for establishing the difference between Medium and High. We propose deleting the second bullet item ("Planning time frame") in the definition, as it makes the analysis much more complicated without substantial BES Reliability benefit. Many entities lack the resources and tools to be able to incorporate power system planning studies into their NERC CIP work. If the "Planning time frame" bullet item is left intact as part of the definition, we would recommend that there be a stated single study timeframe and that studies be completed before a facility goes into service. This allows time to ensure equipment is in compliance. We also propose deleting the third bullet item in the definition ("could hinder restoration to a normal condition"), due to a lack of clarity. The definition of the phrase "normal condition" varies by entity and would bring about a lack of consistency with respect to this definition.
APPA	Disagree	APPA Task Force Comments: High Impact: The definitions of High, Medium and Low Impact must be based on how the industry plans and operates the Bulk Electric or Bulk Power System. Federal Power Act (FPA) Section 215(a)(4) defines "reliable operations" as: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." Bearing this definition in the EPAct in mind, the qualifier of "uncontrolled" should be added to "separation;" in other words, controlled or planned separation is not a High BES Impact. For all practical purposes, the definition of High BES Impact is embedded in the Criteria established in Attachment 1, so, the definition ought to include those criteria. In general, the criteria should be criteria correlated with a threat of an uncontrolled wide-area blackout such as the Northeast Blackouts of 1965 and 2003. The drafting team should consider adding this term along with Medium Impact and Low Impact to the NERC Glossary, since it could possibly be used for more than just this effort. Also, we recommend using the following term found in the NERC Glossary to describe what constitutes a High BES Impact event: "Adverse Reliability Impact" - The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. With regard to "restoration," we recommend that the SDT differentiate between conditions that "prevent" restoration versus merely "hinder" restoration. For a High BES Impact, we ought to be more concerned with "preventing" restoration

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		than “hindering” restoration. The EPAct definition does not address restoration. Each blackstart unit and cranking path ought to be taken in context with the regional restoration plan. Most regional restoration plans have multiple black-start units and cranking paths. Unavailability of any single unit and cranking path is not a “High BES Impact,” whereas loss of several resources may be categorized as “High.” APPA Task Force Suggested Definition: High BES Impact: BES Cyber Systems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable, has a high likelihood of resulting in an Adverse Reliability Impact to the BES.
Consumers	Disagree	We do not agree that there needs to be three different categories of impact. The concept of “Critical” or not, provided the “bright lines” that the SDT seemed to require. This three level approach, which is lacking a fourth, NO IMPACT, level, only seems to make the asset identification and categorization more complex and more subjective. In addition, the proposed changes seem to remove the ability to evaluate the impact the cyber system has on the BES. As proposed, the Cyber System inherits the same Impact Category as the BES Subsystem, so even minimal or no impact cyber systems/assets must be treated with the same requirements (CIP-003 >> CIP-009) as cyber systems that truly could have a substantial impact. This thereby dilutes the attention that should be paid to these critical systems and adds substantial time, effort and cost for compliance. The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Suggestion: Go back to the Critical Asset, Critical Cyber Asset process identified in the previous revisions
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be “merely guidelines” and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the “planning time frame” which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves. Finally, the word “hinder”, which is ambiguous and subjective, should be changed to “prevent”.
MPPA	Disagree	1. The term “unacceptable risk” is undefined, and leaves the definition open for interpretation. 2. This definition does not clearly quantify the difference between a High BES Impact system and a Medium BES Impact system in a manner consistent with Attachment 1. It is recommended that “, categorized in accordance with

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		attachment 1," be inserted in the first line such that it reads as follows: "…BES Subsystems, categorized in accordance with attachment 1, have High BES Impact if …"
Central Lincoln	Disagree	The last bulleted item is not clear. Restoration from what condition? A small local outage? Central Lincoln agrees with the APPA Task Force comments on this definition, and suggest adding the word "uncontrolled" in front of "separation" so that controlled or planned separations are not included.
NERC	Disagree	1. The phrase "unacceptable risk" is subjective, unauditable, and impractical to apply uniformly across entities. Further, it is contrary to the Commission's directive in Order 706 paragraphs 139-156. 2. Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as "contribute to", More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems.
Dominion	Disagree	It is difficult to accept new criteria without understanding the scope and impact of the proposed categories (high, medium and low) and without greater clarification of the details of the CIP-003 – CIP-009 revisions. If the intent of the high, medium and low categories is to establish VSLs and VRFs, such intent should be so stated by the SDT. Otherwise, Dominion suggests using two levels (high/low) as the use of three levels increases complexity without any added benefit. Dominion is also concerned about the use of the following subjective terms "unacceptable risk," "hinder," "could," "would" and other similar terms. All of those terms should be clarified and implemented on an objective basis.
Encari	Disagree	"High BES Impact" is said to be any BES Subsystem that if destroyed, degraded or otherwise rendered unavailable would result in BES separation. The definition appears to include all BES Subsystems since any subsystem that is destroyed would necessarily be separated from the BES. We recommend that "further uncontrolled separation in the BES" replace the term "BES separation."
US ACE – NW	Disagree	Define "hinder" in the statement "could hinder restoration to a normal condition." This is way too vague a statement and is essentially an unmeasurable item. Would a generator that was slow to start for blackstart assistance be fined for "hindering restoration" even though restoration was only slightly impacted? Need to have a definition that is measurable.
SCE	Disagree	SCE believes that the current definition for high impact BES systems does not bring sufficient clarity to the classification process and should be replaced by the criteria identified in Appendix 1 for making such determinations. SCE also requests clarification on certain ambiguous terms. For example, the term "hinder" is ambiguous and overly broad, as it is not defined by any reference to a duration or degree of impact. Similarly, the term "unacceptable risk" is ambiguous, as it is unclear which party's assessment of risk will be respected. Finally, the duration of the "planning time frame" is unclear.
USBR	Disagree	It is not appropriate to classify an element as high in planning environment which is subject to numerous state condition assumptions. If the categorization is to be the result of a study, the sate conditions needs to be clearly defined. This term

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		is not needed as High or Medium indicated an impact which would be sufficient to warrant analysis of associated cyber asset impacts. The term unacceptable risk should be eliminated as it is not defined in either how it is determined or the criteria of what would be considered unacceptable. The sentence addresses the potential without indicating a risk level.
Dyonyx	Disagree	It is recommended that the phrases “in a planning time frame” and “could hinder restoration” be specifically defined. These phrases add too much subjectivity to the definition without further detailed explanations. Lastly, we believe the term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
Westar	Disagree	The phrase 'they could' in the first and second bullets is vague and leaves open room for interpretation. Suggest removing the phrase. 'could hinder restoration to a normal condition' - What is a normal condition? Need to clarify. Is it all lines, generators and load restored? Suggest either removing it or clarifying. Possibly tie to the 'cranking paths'.
Green Country	Disagree	A single event that will cause an Adverse Reliability Impact to the BES and cannot be stopped with an automatic protection system and/or manual operator intervention.
Oregon PUC		The terms “unacceptable risk of …” and “could hinder restoration” have too much latitude for interpretation by the various responsible entities and auditors. Clear, specific and technically defensible language is needed for this definition.
Manitoba 1	Agree	

Organization	Yes or No	Question 1.g. Comment (Response page 11)
Portland GE	Disagree	This definition is too broad and subjective terms such as “hinder” and “contribute” are not defined. In addition, the requirement does not contain a definition for “unacceptable risk,” which is subjective to each company – and to each auditor - therefore creating an inherent compliance risk. Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” This not only creates confusion, but may also then default everything into a “High” categorization, which would clearly contradict the intent behind the proposed risk framework. Clear, specific, and technically defensible language is needed for this definition. From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required to be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is not an appropriate assumption. It is possible to have cyber systems which, if lost, degraded or compromised, will have no significant impact (or no impact at all, in some cases) in the function, operation or security of the BES subsystem that they support. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem.
PSEG		Comment #1: We do not agree with the use of the phrase “when destroyed, degraded”, because it does not align with the definition of BES Cyber System. BES Cyber System identifies a system compromised by an electronic means while “destroy” and “degraded” generally refer to a physical means of compromise (i.e. hammer, bomb or shotgun). Comment #2: We believe that more definition is needed for the term “planning time frame”. Is this intended to cover planned system outages, upgrades, additions and replacements? Comment #3: We believe that this reintroduces the concept of acceptable risk which was removed in CIP-002. Comment #4: We believe that more explanation of the term “cascading” is needed. Comment #5: We believe that any PM actions, projects, or system modifications could potentially hinder restoration to a normal condition. Comment #6: We believe that distinction should be made between “normal” condition and “operating” condition. Suggestion: “A Transmission or Generator Subsystem compromised through its BES Cyber System which could result in instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies). ” We do not believe that a planning time-frame is needed because the above definition would apply when performing engineering assessments in both the operational and planning time horizons. Restoration Issue: We also believe that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Restoration requirements should be consider separately in Attachment 1. We make this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis following a blackout event is completely different then analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments if the SDT disagrees with our suggestion: We are unclear as what the SDT means by the phrase “emergency, abnormal or restorative conditions, directly cause, contribute to, or create an unacceptable risk”. Although these individual terms may portray a sense of what the SDT is looking for they do not convey enough details for an entity to determine the performance level that needs to be prevented. - What criteria or threshold is applied to conclude “contribute to”? - What considerations should an entity use to identify “unacceptable” risk? - What is an “emergency” for the purpose of this standard? - Does “abnormal” mean any state other then all facilities in service? We believe that our suggested modifications provide a meaningful mechanism for entities, who wish to perform engineering analysis on those facilities listed in Attachment 1, to determine if a facility (Transmission Subsystem or Generation Subsystem) should remain in the identified category level (High or Medium) or be moved to a different category level (High, Medium or Low).
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. In addition, Wisconsin Electric Power Company feels the NERC glossary term Cascading should be used. Also, the term "planning time frame" is not clearly defined. Does this mean we have to make a new assessment for every unit outage and line outage? Wisconsin Electric Power Company recommends removing the language around the planning time frame.
Idaho Power	Disagree	“hinder restoration” is too vague. There are many things that can hinder but not prevent restoration that would not be

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		considered high impact.
SOCO	Disagree	Is the first bullet point intended to refer to an Operational time frame (since the second refers to the Planning time frame)? If that's the case, there will be times in light load periods, when multiple lines are out for maintenance, when the next outage could cause BES reliability concerns. This may not be the case for the exact same area of the system in the Planning time frame. Therefore, in the operations time frame, how would one identify and protect the specific subsystems when they might change on a daily basis? There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each and let those be the definitions and not have them up front at all. This is a standard whose sole purpose is to categorize cyber systems according to their impact on the BES so we can properly secure them. From V1 to now we've had to indirectly determine a cyber system's impact to the BES. We can't take into account any characteristics of the cyber system when we determine its BES impact. The standard requires that if a generation subsystem is high impact then all its associated cyber systems are high impact regardless of their actual impact to the generation subsystem. This will result in classifying most cyber systems higher than their actual impact. One suggestion is to determine the cyber system's impact directly against criteria similar Attachment 1. In essence ask "what is this cyber system's span of control?" and classify cyber systems based on how much of the BES they can control and adversely affect. A high impact cyber system can affect 10,000 MW's of generation or more than 50 transmission paths; etc. Under the definition for Medium BES Impact, we need to understand the difference between "directly cause" (shown in the High Impact) and "directly affect" (shown in the Medium Impact). If there is no difference, we suggest that the bullet points be introduced the same for both. Definition of High BES Impact – need a better understanding of what is meant by "could hinder restoration to a normal condition"; is the restoration to a normal condition directed toward a blackstart situation? Loss of a Transmission Subsystem could leave the power system in an abnormal state for an extended period of time (days/weeks) but does not mean that this situation is an unacceptable risk of instability, separation, or cascading failures. Loss of communication with a substation RTU (of a High BES Impact Transmission Subsystem) may hinder restoration to a normal condition should the need arise to control via the RTU while communication is down. We hope that this is not what was intended by the phrase "could hinder restoration to a normal condition". This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions.
DTE	Disagree	We are concerned that the term "unacceptable risk" is reintroducing the "acceptance of risk" concept that was removed from previous versions. The drafting team needs to define "planning time frame".
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	It is recommended that the phrases “in a planning time frame” and “could hinder restoration” be specifically defined. These phrases add too much subjectivity to the definition without further detailed explanations. Lastly, we believe the term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	N&ST is concerned that the phrase, "unacceptable risk" may be frequently subject to interpretation. In addition, what group or groups would make such a determination?
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	E ON U.S. recommends deleting the section: Any number of emergency or abnormal conditions, undefined as those situations are, could result in a situation in which nearly any BES subsystem could “contribute” to creating an unacceptable risk. The scenarios are only limited by one’s imagination. More objectivity is required in order to provide reasonable limits to the analyses.
Carthage	Agree	
WECC	Disagree	We feel this definition does a good job of defining situations that are a high impact to the BES, however, it continues to provide open ended language such as “could directly” that does not provide adequate clarity on if something should be

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		considered an impact or not. What does contribute to or cause unacceptable risk mean? How is unacceptable judged? What was the intent of the term “planning time frame”?
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a. CenterPoint Energy believes the “Critical Asset” definition in the current version of CIP-002 should be retained. However, CenterPoint Energy would support the SDT incorporating the proposed characteristics of “High BES Impact” into the requirements or definition of “Critical Assets” in version 4. Likewise, some of the concepts found in Attachment 1 could be useful for putting some more specificity into the risk based assessment methodology for determining Critical Assets. However, Attachment 1 would need some refinement. Please refer to CenterPoint Energy’s comments to question 8.
LCRA	Disagree	The “planning time frame” needs to be defined.
FRCC	Disagree	This also uses the term "degraded" which is ambiguous. See previous comment. In addition, the first bullet uses the terms "unacceptable risk". Who determines what is unacceptable? This is not easily monitored by compliance enforcement authorities and would likely lead to interpretation requests. If the drafting team has knowledge of what they consider to be unacceptable, they should clearly state it. The first bullet has includes "BES" instability, and "BES" separation, why do the sub-bullets in the planning time frame not refer to "BES" ?
NIPSCO	Disagree	We believe that more clarity is needed for the term “planning time frame”. Is this intended to cover planned system outages, upgrades, additions and replacements? An entity could interpret any maintenance actions, projects, or system modifications could potentially hinder restoration to a normal condition. Additionally, we believe that this reintroduces the concept of acceptable risk which was removed under FERC order 706. Suggestion: Clarify the intent of the term planning time frame and remove references to unacceptable risk.
ConEd	Disagree	There should be a ‘High BES Impact’ category that deals with Control Center-type systems and then a lower level that deals with Transmission Substations. To place a control center and a substation in the same category level is not in the direction we should be heading. Individual Transmission Substations simply are not as important as area Control Centers.
EEI	Disagree	EEI believes that the current written definition for high, impact BES systems does not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in an (amended) Appendix 1 to make such determinations. Restoration Issue: EEI also believes that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Restoration requirements should be considered separately in Attachment 1. We make this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis following a blackout event is completely different then analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Alternative strategies will need to be identified for entities with flexible blackstart plans, e.g. multiple Blackstart units with multiple cranking paths. Reliability of the BES is not advanced by creating significant compliance liability for those organizations that have already invested in developing a flexible and resilient blackstart strategy. The “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats.
O&R	Disagree	There should be a ‘High BES Impact’ category that deals with Control Center-type systems and then a lower level that deals with Transmission Substations. To place a control center and a substation in the same category level is not in the direction we should be heading. Individual Transmission Substations are not as important as area Control Centers.
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "High BES Impact". The words "contribute to" need to be removed. What is meant by "a cascading sequence of failures"? We suggest that this term should be replaced with "widespread outages". We doubt that SERC, NERC, and FERC would agree on what an acceptable or unacceptable risk would be after an event would have occurred. We believe a MW threshold for load lost should be established that would define a High BES Impact, such as 300 MW other than consequential load, consistent with the threshold for a NERC reportable event under NERC EOP-004 and also the threshold for the DOE Energy Emergency Incident and Disturbance Reporting Requirement per Form EIA-417. Alternatively it would suffice to identify IROL as High BES impact. The last statement in the definition "could hinder restoration to a normal condition" is too broad of a statement for a definition; it needs to be classified as Low or Medium BES Impact. From the perspective of a system restoration from a full blackout condition, the loss of any asset could "hinder" the restoration to a normal condition.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
Black Hills	Disagree	Need definition of "could", "Contribute to", and "unacceptable risk". Current CIP-002-1 guidance is that the probability = 1, therefore "could" will always happen. "planning time frame" needs to be defined. A lot can happen in ten years - which is one of our planning time frames. Is "abnormal" limited to N-3? Need to define "hinder" - how much is of significance?
TNMP	Disagree	TNMP has a concern regarding the current definition. High BES Impact would be defined in the official NERC glossary, and categorized by the criteria in CIP-002 Attachment 1. The definition needs an additional “AND”, not “OR”, bullet statement of “further constrained by the criteria in CIP-002 Attachment 1.” By having a definition and a criteria it gives auditors two places to look to determine impact of a BES Subsystem. Currently, the criteria fail to properly address facilities with joint ownership. Could an auditor use the current definition to help clarify where the criteria is lacking in real world applications? TNMP believes this concern needs to be addressed by the drafting team with certainty. TNMP has experienced auditors and attorneys utilizing strict application of actual standard text, rather than referencing discussions and guidance surrounding development of the standards.
NVEnergy	Disagree	While we appreciate the efforts of the Drafting Team to characterize the qualities of a High Impact Subsystem, as written, these qualities are still excessively vague. For instance, one could easily conclude that any unavailable BES subsystem “could hinder restoration to a normal condition”. What degree of hindrance is specified here? Technically, any abnormal condition represents some hindrance to the restoration of a system to normal condition. As with the existing paradigm of the present CIP RBAM practice, there continues to be a lack of needed specificity in classification of assets/subsystems. The concepts described in this proposed definition appear to have some merit, but the difficulty comes about when the entity goes to make a determination.
MWDSC	Disagree	Unclear who determines what "unacceptable risk" is? Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding the adjective "interconnected" before the term BES under each bullet. For example, "risk of interconnected BES instability" Also, need more specific criteria such as in Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Disagree	Optional definition: A single event that will cause and Adverse Reliability Impact to the BES and cannot be corrected with an automatic protection system and/or manual operator intervention.
NCEMCS	Disagree	"could hinder restoration to a normal condition" - This is an open ended statement and needs a better clarification of the actual conditions. For example, if some condition destroyed all communications at a BES facility but it was possible to restore service manually, this definition could hinder restoration.
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Agree	
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for “BES Impact” such as “BES subsystems that if destroyed, degraded, or otherwise rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines provided in Attachment 1 of this Standard.” Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.
BPA Trans	Disagree	1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this makes sense, but: "BES Cyber Systems need to be “secure” not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", "unacceptable risk," or “hinder restoration.” In particular, what is, and how long is a "planning time frame"? 3. It is unclear why the second and third conditions (bullets) removes the reference to the BES. Is this referring to the BES, a single BES subsystem? There is no way of knowing what the intended referent is. 4. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is “destroyed, degraded or otherwise rendered unavailable.” But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of “Subsystems whose destruction, degradation, or lack of availability could lead to …” The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
Allegheny Supply	Disagree	
KCPL	Disagree	This is too broad with regard to "BES Subsystems". There will always be a "tipping" point of generation and transmission outages, that, when crossed, yields an unreliable and undesirable operating condition. As an example, any combination of generating facilities within the Eastern interconnect that totals half of the generation meeting load demand, if removed from service, would be devastating to the operation of the BES. The way this is written, all generating facilities would have to be included as a HIGH. The same illustration could be used for transmission facilities. In addition, placing the burden of establishing the loss of a facility or group of facilities on the Reliability Coordinators and the reliability impact is a concern as they do not have the resources to manage the likely flood of requests and endless operating configurations that would result from Registered Entities seeking relief from this CIP Standard. If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	The definition, as stated here and without the specific guidance provide in the Standard, provides criteria that most Generation Owners can not determine – but that most Transmission Operators can determine. This exacerbates the issue exiting with the current version of the standards. This noted, the criteria included in the Standard provide a clear set of lines for making the classification. As such, this is acceptable if the definition includes the reference to the criteria as the means to make the determination. What will be the definition of unacceptable risk? What is the reason for further breaking down the BES into these categories (high, medium, low)? Is this to better categorize Critical Assets? More categories do not necessarily benefit Critical Asset determination. Coordination between the GO/GOP and the TOP is currently the main driver for Critical Asset determination. Establishing more categories will likely add another unnecessary level of complexity.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If a new definition is created, the scope should be limited to "direct" causes and exclude "in the planning time frame." Planning timeframe is vague and varies. As proposed, it cannot be consistently implemented or fairly audited. The standard should address the current rating and impact, not a potential future impact.
CPG	Disagree	This definition takes into account BES Subsystems if, when destroyed, degraded or otherwise rendered unavailable could hinder restoration to a normal condition. If this term is used solely with Critical Infrastructure Protection, then why would cyber assets be included in restoration, given that they will most likely not be functioning during a blackout? Furthermore, the term "unacceptable risk" is not well defined. It is vague and needs further defining.
Santee Cooper	Disagree	High impact should be left to be concerned with actual threats of uncontrolled wide area blackouts. This is the most important Impact and it should always be treated as such, and should not have problematic items such as "hindering" or short term risks…When there are viable alternatives to BES problems, such as Blackstart Unit alternate cranking paths,

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		we should not Carte Blanche all Blackstart Units into the High Impact arena. Attachment 1 definitively needs further work. You don't want to trivialize the High Impact, so only those items that have an absolute impact should be on the high impact listings.
OGE	Disagree	• Provide the exact duration of a "planning time frame". • The term "contribute to" is too discretionary. • A metric is needed to know what "unacceptable" or "hinder" means. • Why is the term "BES" excluded in the second bullet above? (BES instability). What is the difference between "BES instability" and "instability"? What is the difference between "BES separation" and "separation"? What is the definition of "instability"? • "Normal condition" needs to be defined in this context. • OPTION: A single event that will cause an Adverse Reliability Impact to the BES and cannot be stopped with an automatic protection system and/or manual operator intervention.
Oncor	Disagree	The enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1. Remove from Definition of Terms section.
PPL Supply	Disagree	Comments: A more precise definition of Black Start generating units is needed that in the proposed Rev. 4. To say that "Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem." is inadequate to identify only those generating units that are used for initial restoration of the BES. System restoration plans normally identify all units from the blackstart initiating through the thermal generation at the end of the cranking path, including any intermediary units, so clarification is needed to avoid misinterpretation.
St. George	Agree	
NGRID	Disagree	Reference to BES Cyber system should be made since the Transmission/Generation subsystems will be degraded or destroyed through BES Cyber System (intent of the standard). Also, it is recommended to consider an alternate phrase/word to "destroyed/degraded" as they are generally referred to a physical means of compromise. "BES Subsystems have High BES Impact if, when "compromised" through its BES Cyber Systems, they could:…" If the SDT decides to keep the current definition, then answers to following questions are required - What criteria or threshold is applied to conclude "contribute to"? - What considerations should an entity use to identify "unacceptable" risk? - What is an "emergency" for the purpose of this standard? - Does "abnormal" mean any state other then all facilities in service?

Organization	Yes or No	Question 1.g. Comment (Response page 11)
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1.
FE	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three BES Impact buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. This High BES Impact definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. For example, it is subjective as to why only a 2000MW and above generation Subsystem threshold would be screened for High BES Impacts. The focus should be evaluating generation Subsystems, regardless of the MW value tripped, that could lead to a High BES Impact result. FE suggests an approach that creates greater clarity and a "bright line" as to what is deemed to be a High BES Impact; meaning that the standard focus only on those threats that could lead to a High BES Impact (cascade, system separation, instability, restoration concerns) and drive greater uniformity in the industry on how we land there. To move beyond that into classifying a Medium BES Impacts and certainly Low BES Impacts is not needed. We also offer a specific edit to the High BES Impact definition. The second bullet is largely redundant to the first bullet, causes confusion and not needed. FE suggests that the second bullet be removed.
TECO	Disagree	The amended Attachment 1 categorization definition (see EEI comments) should be used in place of this, as it is more clearly defined. If that cannot be accomplished, references to the “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a reliable cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. The terms “unacceptable risk”, “abnormal” and “hinder” need to be more clearly defined, to avoid confusion and misinterpretation. Additionally, we support EEI’s comments on restoration issues.
CECD	Agree	Agreement with the definition is based on the registered entity having the independence to define its BES subsystems.
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
GTC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized? The use of the phrase “unacceptable risk” makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase “could … cause” is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase “could hinder” is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose. With respect to the second bullet, it is unclear what is meant and it needs to be clarified.
Xcel	Disagree	The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion. The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1. There is a need to have a definition of “unacceptable”. What criteria do you use to determine if a risk is unacceptable?
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 h, 1i should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. “Cascading Sequence of failures” is not clearly defined In the phrase, “Or could hinder restoration to normal condition”, normal condition is not clearly defined.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		Please clarify what is meant by planning time frame. "Unacceptable risk" not well defined. It is vague and should be linked to NERC transmission planning standards. Also, please note response to Q3.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Regarding "High BES Impact" and "Medium BES Impact" references to the "planning time frame" should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. Consider striking references to "planning time frame" and replace with "based on analysis of real-time operating conditions."
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Disagree	AP believes that the current written definition for high impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations. AP also believes that this reintroduces the concept of acceptable risk which was removed in CIP-002.
FMPA	Disagree	We applaud the SDT in nearly correctly identifying the criteria for which High BES Impact should be determined in alignment with the definition of Reliability in the Energy Policy Act of 2005. The FPA Section 215(a)(4) defines "reliable operations" as: "operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements." This FPA definition is almost synonymous with the definition of Adverse Reliability Impact in the NERC Glossary of terms: "(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection". FMPA recommends using the NERC Glossary to simplify the definition. Bearing this definition in the FPA and Glossary in mind, the qualifier of "uncontrolled" should be added to "separation"; in other words, controlled or planned separation is not a High BES Impact. FMPA recognizes that Adverse Reliability Impact does not address restoration whereas High Impact ought to. However, there is a difference between "hindering" and "preventing" restoration. For a High BES Impact, we ought to be more concerned with "preventing" restoration than "hindering" restoration. Each blackstart unit and cranking path ought to be taken in context with the regional restoration plan. Most regional restoration plans have multiple black-start units and cranking paths. Unavailability of any one is not a "High BES Impact," whereas loss of several may be.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		For all practical purposes, the true definition of High BES Impact is embedded in the Criteria of Attachment 1, so, the definition ought to include those criteria. In general, the criteria should be criteria correlated with a threat of an uncontrolled wide-area blackout such as the Great Northeast Blackouts of 1965 and 2003. Therefore, the definition of “High Impact” would have more clarity by saying: “BES Cyber Systems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable, has a high likelihood of resulting in an Adverse Reliability Impact to the BES, or could prevent restoration efforts.”
Duke	Disagree	This definition is not needed because Attachment 1 of the standard describes High BES Impact in great detail.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for High Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "High?" What if something fit the Criteria for Medium impact but in fact would have the effects of this High definition? How should it be categorized? The use of the phrase “unacceptable risk” makes these definitions highly subjective – what is an unacceptable risk? Who decides this? How does an entity know that their definition is the same as the auditors? The phrase “could … cause” is also excessively vague and subjective. Many things could happen, the question is: would they? What is the probability? The phrase “could hinder” is also excessively broad. For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
IESO	Disagree	The term "risk" is misused in the phrase "unacceptable risk of". the term should refer to the "unacceptable likelihood of"
Manitoba 2	Disagree	This definition very closely resembles the Risk Factors defined in the NERC Reliability Standards Development Procedure, which are used to develop Violation Risk Factors (VRFs), which is redundant, and is not consistent with the impact criteria described in Attachment 1. The definition “High BES Impact” should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. It is unclear what is meant by “in a planning time frame” and this point should be removed. The standard is limited to

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		systems that are already in-service. Please define emergency, abnormal, or restorative conditions. Restoration should be categorized as “Medium BES Impact”. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	ATC does not agree with the use of the phrase “when destroyed, degraded”, because it does not align with the definition of BES Cyber System (Either ATC or the SDT definitions). BES Cyber System identifies a system compromised by an electronic means while “destroy” and “degraded” generally refer to a physical means of compromise (i.e. hammer, bomb or shotgun). Suggestion: “A Transmission or Generator Subsystem compromised through its BES Cyber System which could result in instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies). ” ATC does not believe that a planning time-frame is needed because the above definition would apply when performing engineering assessments in both the operational and planning time horizons. An alternative suggestion would be for the SDT to use the existing NERC Event category. Category 5 event is High Category 5 An event resulting in one or more of the following: a. The loss of load of 10,000 MW or more. b. The loss of generation of 10,000 MW or more. Category 4 event is Medium Category 4 An event resulting in one or more of the following: a. The loss of load from 1,000 MW to 9,999 MW (excluding SPS/RAS as noted in Category 2, UFLS, or UVLS actuation). b. Unintended system separation resulting in an island of a combination of load and generation of more than 10,000 MW. Category 3 event is Low Category 3 An event resulting in one or more of the following:

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		a. The loss of load from 500 MW to 1,000 MW (excluding SPS/RAS, UFLS, or UVLS actuation). b. The unplanned loss of generation (excluding automatic rejection of generation through SPS/RAS as noted in Category 2) of 2,000 MW or more in the Eastern Interconnection or Western Interconnection, and 1,000 MW or more in the Texas or Québec Interconnections. c. Unintended system separation resulting in an island of a combination of load and generation of 5,001 MW to 10,000 MW. Category 1 or 2 is excluded from CIP-003 - 009. Restoration Issue: ATC also believes that the SDT must separate out the issues of restoration following a black out event from the issue of what could cause a black out event. Restoration requirements should be considered separately in Attachment 1. ATC makes this suggestion because the use of restoration Blackstart units and cranking paths are only needed following a blackout event. The engineering analysis following a blackout event is completely different than analysis looking at events that could cause a blackout. Suggestion: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit as high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments if the SDT disagrees with our suggestion: ATC was unclear as what the SDT means by the phrase “emergency, abnormal or restorative conditions, directly cause, contribute to, or create an unacceptable risk”. Although these individual terms may portray a sense of what the SDT is looking for they do not convey enough details for an entity to determine the performance level that needs to be prevented. - What criteria or threshold is applied to conclude “contribute to”? - What considerations/criteria should an entity use to identify “unacceptable” risk?

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.g. Comment (Response page 11)</th></tr>
<tr><td></td><td></td><td>

- What is an “emergency” for the purpose of this standard?
- Does “abnormal” mean any state other than all facilities in service?

ATC believes that our suggested modifications provide a meaningful mechanism for entities, who wish to perform engineering analysis on those facilities listed in Attachment 1, to determine if a facility (Transmission Subsystem or Generation Subsystem) should remain in the identified category level (High or Medium) or be moved to a different category level (High, Medium or Low).

</td></tr>
<tr><td>LES</td><td>Agree</td><td>

We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
</table>

</td></tr>
</table>

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		<table><tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr></table> Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
PSE	Disagree	The definition should focus on the level of disturbance the BES Subsystem could cause if destroyed or degraded. It is unclear what "in a planning time frame" is intended to mean. Further Puget Sound Energy supports EEI's comments relative to exclusion of restoration activities included black start generation and cranking paths for reasons 1) not all entities need or have blackstart units, 2) they could be identified for local customer support versus interconnection support and 3) the complexity associated with the flexibility in cranking that a restoration plan must address due to the varying scenarios that could occur which makes it difficult to determine one or two critical paths.
IMPA	Disagree	The Standard and Attachment 1 both define what constitutes a High BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a High BES Impact. In addition, the definition needs to be removed because it uses the term “unacceptable risk” which could have various meanings depending on an individual’s judgment.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO comments. In the 1st bullet, ERCOT ISO requests clarification of “unacceptable risk”. This is a very ambiguous requirement and lends itself to subjective interpretation by the Responsible Entity and an audit body. Recommend that the drafting team consider returning to the use of the definition of Adequate Level of Reliability in determining risk tolerance. ERCOT ISO recommends removing the 2nd bullet or at least differentiating between operating and system planning time horizons. Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706.

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		The second bullet of the definition is largely redundant to the first bullet and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. If the second bullet is omitted, the reference to “restoration” will need to be moved to the first bullet. Furthermore, this definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 1 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
PacifiCorp	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES Subsystems that may have a high impact in the planning time frame. The standard should address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The High BES Impact definition appears to mimic the definition of a High Violation Risk Factor. We question why there is a need to consider “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation.
PEPCO	Disagree	The current definition for High BES Impact does not bring sufficient clarity for determining the appropriate category. There needs to be a bright-line between High BES Impact, Medium BES Impact, and Low Impact. For High Impact, it appears to be risk based. How are BES instability, BES separation, and a cascading sequence of failures pre-determined or defined? Could all BES systems hinder restoration to a normal condition? What is meant by hinder or normal condition? More clarity is need for the term “planning time”. Differentiating between High, Medium and Low BES Subsystems may have little value or credibility for associated cyber security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. We suggest the following: Do not use High, Medium, or Low. If cyber control system first approach is use, we would offer that the high, medium, or

Organization	Yes or No	Question 1.g. Comment (Response page 11)
		low would not be needed. Appropriate security measures/requirements would be based on platform of in-scope BES cyber control systems, the connectivity of the asset (TCP/IP vs. dial-up vs. not connected), and/or the span of control of the cyber asset's impact. If the SDT feels that this term is still required, suggest the you use only the criteria identified in an (amended) Appendix 1 for the definition.
NEI	Disagree	A) In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three BES Impact buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. This High BES Impact definition does not match the current examples/criteria included in Attachment 1 that supposedly correspond to this definition. The examples in Attachment 1 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. For example, it is subjective as to why only a 2000MW and above generation Subsystem threshold would be screened for High BES Impacts. The focus should be evaluating generation Subsystems, regardless of the MW value tripped, that could lead to a High BES Impact result. NEI suggests an approach that creates greater clarity and a "bright line" as to what is deemed to be a High BES Impact; meaning that the standard focus only on those threats that could lead to a High BES Impact (cascade, system separation, instability, restoration concerns) and drive greater uniformity in the industry on how we land there. To move beyond that into classifying a Medium BES Impacts and certainly Low BES Impacts is not needed. B) We also offer a specific edit to the High BES Impact definition. The second bullet is largely redundant to the first bullet, causes confusion and not needed. NEI suggests that the second bullet be removed. C) Since cyber security is not the focus here, this has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security. D) It is recommended that Attachment 1 (as modified by comment A)) be used to provide an adequate definition, and that the Glossary be point to the Attachment. E) If the definition is to be kept, provide clarification for the terms "unacceptable risk" and ""could hinder". F) Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the Appendix). While the current "one size fits all" approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

Summary Consideration: There were many comments on the need for definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1. The SDT reviewed them and has removed these definitions.

Many also commented on the absence of a "No Impact" category. It is the SDT's opinion that the definition of BES Cyber Systems effectively removes Cyber Systems with no impact from the scope, and that a BES Cyber System has some level of impact, by definition.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Progress Energy	Disagree	Keep only the 2nd bullet as-is. Remove 1st bullet "directly affect the electrical state or the capability of the BES;" – it is too vague and would cause varying interpretations. Remove 3rd bullet "in a planning time frame, under emergency, abnormal, or restorative conditions, – directly affect the electrical state or the capability of the BES; or – directly affect the ability to effectively monitor and control the BES." – Scope of CIP standards should only address real-time cyber operations.
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The third bullet of the definition is largely redundant to the first two bullets and improperly references "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". This is not reasonable and this definition needs to be revised significantly.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
GSOC/OPC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Hayden	Disagree	This is a confusing definition. The term "...directly affect..." can also be applied to the definition of "HIGH BES Impact." As such, I wonder if this can be rewritten to help place the impact on the right layer of the impact continuum. Can it be more specifically related to the BES Adequate Level of Reliability (ALR) requirements? This definition would be very difficult to enforce with the current level of criteria.
SDGE	Disagree	In addition to the lack of a “risk statement” in this “Medium BES impact” definition, what is the difference between, “causing, contributing to, or creating, unacceptable risk to the BES” (in “High impact”) and “directly affecting the electrical state or capability of the BES” (in “Medium impact”)? Why is the risk of something happening to the BES deemed a higher impact than “directly affecting” the BES? This definition for “Medium” doesn’t provide much granularity or difference between that of “High BES impact”. We propose a more binary approach with respect to BES impact, namely having “BES impact” and “no BES impact” choices (re-working the “high impact” and “low impact” definitions). Currently, the way the three different impact choices are defined (H, M, L), will unnecessarily complicate drafting and implementing the CIP-003 through CIP-009 Standards. For example, would requirements for access to “High BES impact” assets be different than the requirements for access to “Medium BES impact” assets? Would information associated with high impact BES Subsystems have different requirements than information associated with medium impact BES Subsystems? Would training requirements be different for the aforementioned BES classifications? Would vulnerability assessments be lesser in scope or less frequent in occurrence for medium impact BES classifications versus that of high impact BES classifications. This imprecision would confuse implementation and increase the administrative cost of compliance without increasing BES security. We are proposing having just two choices for BES Impact (BES Impact, and no BES Impact).
APPA	Disagree	APPA Task Force Suggested Definition:

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Medium BES Impact: BES Cyber Systems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could cause a post-contingency system state in which an additional single contingency is likely to result in an Adverse Reliability Impact to the BES.
Consumers	Disagree	If the SDT is unwilling to return to the Critical Asset, Critical Cyber Asset process identified in the previous revisions, then this category should be renamed "Low" impact, and the currently proposed low impact should be re-identified as "No Impact". This would allow the SDT and REs to focus on assets and cyber systems that truly have an impact and dismiss those that do not.
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be "merely guidelines" and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the "planning time frame" which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves.
MPPA	Disagree	1. This definition could be equally applied to High BES Impact. A system that can affect the electrical state of capability of the BES, could impact the stability of the BES, there by falling under the definition of a High BES Impact. 2. This definition does not clearly quantify the difference between a High BES Impact system and a Medium BES Impact system in a manner consistent with Attachment 1. It is recommended that ", categorized in accordance with attachment 1," be inserted in the first line such that it reads as follows: "…BES Subsystems, categorized in accordance with attachment 1, have Medium BES Impact if …"
Central Lincoln	Agree	
NERC	Disagree	Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as "contribute to", and "create an unacceptable risk". More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems.
Dominion	Disagree	Dominion does not agree with including the statements "directly affect the electrical state or the capability of the BES" and "directly affect the ability to effectively monitor and control the BES" in the definitions of "Medium BES Impact" and "Low BES Impact." Every physical generation or transmission asset has the ability to directly affect the electrical state or the capability of the BES. Therefore, by default, all such assets would all be classified as Medium BES Impact. To the extent these devices are monitored, each directly affects the ability to effectively monitor the BES. The term "electrical state" should be clarified.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Encari	Disagree	"Medium BES Impact" is said to be any BES Subsystem that if destroyed, degraded or otherwise rendered unavailable could directly affect the electrical state or the capability of the BES. The definition appears to include all BES Subsystems since any subsystem that is destroyed would necessarily affect the capability of the BES. We recommend that "adequate level of reliability" replace the term "capability." "Adequate level of reliability" of the BES is a term with an established meaning. NERC defined the term "Adequate level of reliability" on May 5, 2008 in a filing with FERC.
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the current definition for medium impact BES systems does not bring sufficient clarity to the classification process and should be replaced by the criteria identified in Appendix 1 for making such determinations. SCE also requests clarification on certain ambiguous terms. For example, it is unclear to SCE what the meaning of "electrical state" is, as that term is not defined in the NERC Glossary of terms. The duration of the "planning time frame" is also unclear.
USBR	Disagree	The term "electrical state or capability" it too vague to help determine what is a medium impact. It would be better relate the medium state to the terms used in high with a degree of separation. This term could imply that any change in the BES irrespective of the durability of the BES under those conditions would be a medium impact. This would mean that any event would be considered a medium impact irrespective of the true reliability of the BES immediately following the event.
Dyonyx	Disagree	The proposed definition uses undefined terms ("electrical state", "planning time frame") and is too subjective. In addition, we do not believe the term "capability" is appropriate. The loss of even 10 MW will impact the total "Capability" of the regional system, but this is not the intent of the standard.
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The third bullet of the definition is largely redundant to the first two bullets and improperly references "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation. In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES". This is not reasonable and this definition needs to be revised significantly. Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
Westar	Disagree	Again the phrase 'they could' is vague. Suggest removing. The first bullet is very vague. What is meant by 'directly affect the capability of the BES'. We need this more clearly defined.
Green Country	Disagree	A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES.
Oregon PUC	Disagree	The language “could directly affect …” seems overly broad. Clear, specific and technically defensible language is needed for this definition.
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree with this definition, and incorporates by reference the same comments as for the High BES Subsystem definition. This definition is too broad and subjective terms such as “hinder” and “contribute” are not defined. In addition, the requirement does not contain a definition for “unacceptable risk,” which is subjective to each company – and to each auditor - therefore creating an inherent compliance risk. Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” Finally, there is not a clear delineation between the High impact “directly cause” and Medium impact “directly affect.” This not only creates confusion, but also may then default everything into a “High” categorization, which would clearly contradict the intent behind the proposed risk framework. Clear, specific, and technically defensible language is needed for this definition. From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-002-4 Attachment 1) for categorization criteria. This is not an appropriate assumption. It is possible to have cyber systems which, if lost, degraded or compromised, will have no significant impact (or no impact at all, in some cases) in the function, operation or security of the BES subsystem that they support. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem.
PSEG	Disagree	Comment #1: The phrases “directly affect”, “electrical state” and “effectively monitor” does not convey sufficient clarity for entities to properly identify BES Subsystem which should fall into this category. We offer the following three options for the SDT to consider: b) Delete this classification and keep only the “High” and “Low” classifications. c) Provide more specificity to the term in order for entities to understand what is the potential impact of facilities

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		classified as "Medium". d) Do not define the term Medium BES Impact but identify those facilities that fall under this classification level. (Allow entities to use the same engineering assessment identified for "High BES Impact" to determine if the facilities should be moved to either "high" or "Low". Option 1: This option allows the team to focus on those BES Cyber Systems that truly have a high impact on the BES. Option 2: If the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could directly affect the electrical state or capability of the BES? - Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?) - See our comments under High BES Impact for the phrase "under emergency, abnormal, or restorative conditions". Option 3: This would eliminate the need for the SDT to define Medium BES Impact and allow entities the options to use an engineering assessment to either raise or lower those BES Cyber Systems that have been identified in Attachment 1. Example: If an entity could demonstrate through an engineering assessment that a facility identified as Medium BES Impact would not cause instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies) then that facility could be identified as "Low". Comment #2: We fail to see the difference between "directly affect the electrical state or the capability of the BES" in Medium BES Impact and the first bullet in High BES Impact.
WE-Energies	Disagree	Wisconsin Electric Power Company feels there should be additional information provided as to what "electrical state or capability" means. This should include how this risk level would actually impact the BES. In addition, Wisconsin Electric Power Company agrees with EEI's comments regarding this definition.
Idaho Power	Disagree	Too vague. Every BES Subsystem has some affect on the electrical state of the BES. Too much room for subjectivity on what directly or indirectly affects the BES.
SOCO	Disagree	There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each and let those be the definitions and not have them up front at all. Under the definition for Medium BES Impact, we need to understand the difference between "directly cause" (shown in the High Impact) and "directly affect" (shown in the Medium Impact). If there is no difference, we suggest that the bullet points be introduced the same for both.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Definition of Medium BES Impact – need a better understanding of what is meant by “directly affect the electrical state or capability of the BES” and “directly affect the ability to effectively monitor and control the BES”. The phrase “directly affect the ability to effectively monitor and control the BES” seems to apply more to a Cyber System rather than a BES Subsystem. It is the Cyber Systems that allow the ability to monitor and control the BES not the BES Subsystems themselves. This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions.
DTE	Disagree	The drafting team needs to define “planning time frame”.
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a “No BES Impact” should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	The proposed definition uses undefined terms (“electrical state”, “planning time frame”) and is too subjective. In addition, we do not believe the term “capability” is appropriate. The loss of even 10 MW will impact the total “Capability” of the regional system, but this is not the intent of the standard.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	It is not clear to us what distinguishes "directly affect the electrical state or capability of the BES" from the previous (High) impact definition.
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	Under emergency or abnormal conditions, undefined as those situations are, nearly any BES subsystem could “contribute” to creating an unacceptable risk. The scenarios are only limited by one’s imagination. More objectivity is

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		required. E ON U.S. again recommends deleting the planning time frame bullet and sub-bullets.
Carthage	Agree	
WECC	Disagree	This does not provide additional clarity. See previous comment (1.g).
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a. It is particularly hard to imagine what rationale there would be for attempting to distinguish medium and low impact facilities (setting aside the “subsystem” quagmire). Virtually any non-radial asset, if damaged, would affect the “electrical state” of the BES by, if nothing else, removing one or more network elements. Likewise, one could argue that loss of a single telemeter, let alone an entire unit at one substation, directly affects the ability to monitor and control the BES, although one could argue about the meaning of “effective” monitoring and control. If the basic intent of the SDT is to apply some set of requirements for every cyber asset, regardless of criticality, the SDT should simply propose such a set of requirements rather than introducing this proposed paradigm.
LCRA	Disagree	1. The “planning time frame” needs to be defined. 2. The phrase “directly affect” should be changed to “directly and adversely affect”. The original phrase is too broad.
FRCC	Disagree	See previous comments on use of the term "degraded". In addition, the first bullet uses the terms "electrical state" or "capability" of the BES . These terms are very broad and can mean a number of different things to different people. It should be clear what is expected here.
NIPSCO	Disagree	We believe there is not enough distinction between High and Medium BES impact. There appears to be overlap within the definitions and this overlap will create confusion and a variety of interpretation issues. Suggestion: Review the definitions of High and Medium and provide an increased distinction between the two criteria.
ConEd	Agree	
EEI	Disagree	EEI believes that the current written definition for medium impact BES systems does not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in an (amended) Appendix 1 to make such determinations.
O&R	Agree	
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of Medium BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "Medium BES Impact". This definition is again too broad, to what order of magnitude to "directly affect the ability/electrical state" refer. The loss of any asset or subsystem would affect the BES but

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		to varying magnitudes. An explanatory statement should be added such as "directly affect the electrical state or capability of the BES to maintain established voltage conditions within 3% of normal system conditions." We believe that we need a MW threshold for load lost that would qualify for Medium BES Impact, such as more than 100 MW but less than 300 MW other than consequential load.
Black Hills	Disagree	Need definition of "could". Current CIP-002-1 guidance is that the probability = 1, therefore "could" will always be a possibility. "planning time frame" needs to be defined. A lot can happen in ten years - which is one of our planning time frames. Concern about meaning of "directly" as compared to "indirectly" - what is the significance? Definition of "capability of the BES"?
TNMP	Disagree	Comments on High BES Impact are equally applicable to this definition.
NVEnergy	Disagree	As with the above “High Impact” comments, the same applies here as well. Beyond that, the term “directly affect the electrical state” is not sufficiently descriptive in our view. ANY destroyed subsystem necessarily affects the electrical state of the BES, so we don’t think this provides the degree of clarity needed to classify the applicable subsystems.
MWDSC	Disagree	Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding the adjective "interconnected" before the term BES under each bullet. For example, "directly affect the electrical state or the capability of the interconnected BES;" Also, need more specific criteria such as in Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Disagree	Optional definition: A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Disagree	The wording in the definition that states "directly affect" is too ambiguous to apply this criteria. Suggested wording for bullet #1 is " results in a violation of the Transmission Operator's operating criteria." Suggested wording for bullet #3, first sub-bullet is "results in a violation of the Transmission Operator's planning criteria."
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for “BES Impact” such as “BES subsystems that if destroyed, degraded, or otherwise rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		provided in Attachment 1 of this Standard." Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.
BPA Trans	Disagree	Some of our comments for High BES Impact are applicable and are repeated here: 1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this makes sense, but: "BES Cyber Systems need to be "secure" not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-00204 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", etc. In particular, what is, and how long is a "planning time frame"? 3. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is "destroyed, degraded or otherwise rendered unavailable." But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of "Subsystems whose destruction, degradation, or lack of availability could lead to …" The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. Additionally, 4. The verb "affect" is too broad. The Standard does not state that the effect must be harmful. Even if we assume that what is really meant is "affect adversely", we need to define how much is enough. For example; if a print server generates weekly summary reports, then its absence would directly and adversely affect the "ability to monitor… the BES". That would erroneously make it a Medium BES impact. Note that FIPS-199 uses "significant adverse effect" for Moderate Impact, which is the equivalent of Medium Impact in this standard. Question, Why not use "Moderate Impact", instead of "Medium"? FIPS-199 is required for use by Federal agencies and is

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		commonly used elsewhere. It may be sensible to use the same terminology. We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
Allegheny Energy		Medium BES Impact • in a planning time frame, under emergency, abnormal, or restorative conditions, - directly affect the electrical state or the capability of the BES; or - directly affect the ability to effectively monitor and control the BES. “Planning time frame" needs to be better defined
KCPL	Disagree	This is too broad. There will always be a “tipping” point of generation and transmission outages, that, when crossed, yields an unreliable and undesirable operating condition. As an example, any combination of generating facilities within the Eastern interconnect that totals half of the generation meeting load demand, if removed from service, would be devastating to the operation of the BES. The way this is written, all generating facilities that was not included as HIGH would have to be included as a MEDIUM. The same illustration could be used for transmission facilities. In addition, placing the burden of establishing the loss of a facility or group of facilities on the Reliability Coordinators and the reliability impact is a concern as they do not have the resources to manage the likely flood of requests and endless operating configurations that would result from Registered Entities seeking relief from this CIP Standard. If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	See comments for 1.g above.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If a new definition is created, the scope should be limited to “direct” causes and exclude “in the planning time frame.” Planning timeframe is vague and varies. As proposed, it cannot be consistently implemented or fairly audited. The standard should address the current rating and impact, not a potential future impact.
CPG	Disagree	This definition takes into account restorative conditions, which are included under the term High BES Impact.
Santee Cooper	Disagree	See comments above, once you rework High BES Impact, the Medium and Low will change as well.
OGE	Disagree	• The terminology is too vague. Any line outage would affect the capability of the BES. • What is meant by the term “electrical state”? Is there a definition for that? What is meant by the term “capability”?

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		Is there a definition for that? • OPTIONS: A single event that will require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES. A post single contingency state in which an additional single contingency may require action by an automatic protection system and/or manual operator intervention to avoid an Adverse Reliability Impact to the BES. (N-2?)
Oncor	Disagree	The enforceable definition of Medium BES Impact is actually set by CIP-002 - Attachment 1. Remove from Definition of Terms section.
PPL Supply	Disagree	Comments: Agree with EEI Comments.
St. George	Agree	
NGRID	Disagree	Please elaborate on “electrical state or capability of the BES”. National Grid also recommends considering only bullet 2 – directly affect the ability to effectively monitor and control the BES Reference to BES Cyber system should be made since the Transmission/Generation subsystems will be degraded or destroyed through BES Cyber System (intent of the standard). Also, it is recommended to consider an alternate phrase/word to “destroyed/degraded” as they are generally referred to a physical means of compromise. “BES Subsystems have Medium BES Impact if, when “compromised” through its BES Cyber Systems, they could:…” If the SDT wants to keep this definition then they need to provide more clarity as to which BES Cyber Systems will be included in this category and What are the parameters to determine if a BES Cyber System could directly affect the electrical state or capability of the BES?
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1.
FE	Disagree	We do not support a review/classification of Medium BES Impact threats and therefore disagree with the inclusion of this definition. In addition, this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not "affect the electrical state or the capability of the BES".
TECO	Disagree	The amended Attachment 1 categorization definition (see EEI comments) should be used in place of this, as it is more clearly defined. If that cannot be accomplished, references to the “planning time frame” should be removed.
CECD	Agree	Agreement with the definition is based on the registered entity having the independence to define its BES subsystems.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.
GTC	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
Xcel	Disagree	Comments: See 1.h. In general, we believe the Attachment defines Low, Medium and High and these should be removed from the reference section.
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 g, 1i should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. We feel that the bullet, “directly affect the electrical state or the capability of the BES;” should be removed. The statement is too broad. This also applies to the next to last bullet. Please clarify what is meant by planning time frame? Also, please note response to Q3.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Same as previous (Regarding “High BES Impact” and “Medium BES Impact” references to the “planning time frame” should be removed. Planning involves too many variables to be a reliable estimation of whether a Transmission or Generation Subsystem poses a cyber security threat in real-time. By definition the planning time frame relies on assumptions of load growth and future (e.g. unrealized) transmission and generation projects that are not adequate representations of present day real-time operations. For generators any number of conditions may exist in the planning time frame which would require remediation by either the Transmission Owner or the Generator Owner, but these conditions are only potentialities and not actual threats. Consider striking references to “planning time frame” and replace with “based on analysis of real-time operating conditions.”)
TAPS		See TAPS response to Question 1.a.

Organization	Yes or No	Question 1.h. Comment (Response page 12)
Allegheny Power	Disagree	AP believes that the current written definition for medium impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations.
FMPA	Disagree	The definition of Medium Impact is too nebulous and ambiguous. If a transducer goes out of calibration, is that enough to "directly affect the ability to effectively monitor"? We hope that is not the intent of the SDT. Criteria needs to be associated with this definition to make it useful. This is done in the criteria of Attachment 1, so, really, the true definition of Medium BES Impact is in the Criteria of Attachment 1. To add clarity, FMPA suggests incorporating the concept of being dangerously close to an Adverse Reliability Impact, e.g., only a single contingency away, as determining whether a cyber system has medium impact. FMPA suggests: "BES Cyber Systems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could cause a post-contingency system state in which an additional single contingency is likely to result in an Adverse Reliability Impact to the BES, or could hinder restoration efforts"
Duke	Disagree	This definition is not needed because Attachment 1 of the standard describes Medium BES Impact in great detail.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	How do these definitions of Impact levels relate to the specific Criteria for such levels on Attachment 1? What if something meeting some Criteria for Medium Impact on Attachment 1 did not actually fit this definition? Should it still be categorized "Medium?" What if something fit the Criteria for High impact but in fact would have the effects of this Medium definition? How should it be categorized? For the purposes of a Standard, the objective nature of the Criteria is preferable to the potentially subjective nature of these definitions. Therefore the definition would be better served by simply referencing the criteria identified in Attachment 1. It is difficult to assess whether these definitions (or the Criteria) meaningfully establish a way to apply security "commensurate" with the risk, without having any idea of what different "levels" of particular security measures the standards might impose.
IESO	Disagree	Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we've got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): a. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. b. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined according to studies or other criteria determined by the RC. c. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		compliance.
Manitoba 2	Disagree	This definition very closely resembles the Risk Factors defined in the NERC Reliability Standards Development Procedure, which are used to develop Violation Risk Factors (VRFs), which is redundant, and is not consistent with the impact criteria described in Attachment 1. The definition "Medium BES Impact" should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. It is unclear what is meant by "in a planning time frame" and this point should be removed. The standard is limited to systems that are already in-service. Please define emergency, abnormal, or restorative conditions. Please define "electrical state or capability" of the BES. As currently written, BES Subsystems which have a High BES Impact would also be categorized as Medium BES Impact. Please include a statement indicating that the Medium BES Impact is exclusive of the High BES Impact. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
ATC	Disagree	The phrases "directly affect", "electrical state" and "effectively monitor" does not convey sufficient clarity for entities to properly identify BES Subsystem which should fall into this category. We offer the following three options for the SDT to consider: 1. Delete this classification and keep only the "High" and "Low" classifications. 2. Provide more specificity to the term in order for entities to understand what is the potential impact of facilities classified as "Medium". 3. Do not define the term Medium BES Impact but identify those facilities that fall under this classification level. (Allow entities to use the same engineering assessment identified for "High BES Impact" to determine if the facilities should be moved to either "high" or "Low". Options 1: This option allows the team to focus on those BES Cyber Systems that truly have a high impact on the BES. Option 2: If the SDT wants to keep this definition then they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could directly affect the electrical state or capability of the BES?

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.h. Comment (Response page 12)</th></tr>
<tr><td></td><td></td><td>
- Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
- See our comments under High BES Impact for the phrase “under emergency, abnormal, or restorative conditions”.

Option 3: This would eliminate the need for the SDT to define Medium BES Impact and allow entities the options to use an engineering assessment to either raise or lower those BES Cyber Systems that have been identified in Attachment 1.

Example: If an entity could demonstrate through an engineering assessment that a facility identified as Medium BES Impact would not cause instability, separation or cascading, as defined by the Registered Entity, beyond an entities service territory(ies) then that facility could be identified as “Low”.

(Please see our comment to question 1e)
</td></tr>
<tr><td>LES</td><td>Agree</td><td>
We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.h. Comment (Response page 12)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>Same comments regarding the third bullet as mentioned in 1.g (the complexity associated with the flexibility in cranking that a restoration plan must address due to the varying scenarios that could occur which makes it difficult to determine one or two critical paths). It is unclear what "affect" means in all three bullets. The loss of functionality is planned for per the Reliability Standards so it is unclear if this deems all diversified BES Subsystems that are established to meet this intent must be treated as Medium or just the "backup" BES Subsystem.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The Standard and Attachment 1 both define what constitutes a Medium BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a Medium BES Impact.</td></tr>
<tr><td>ERCOT</td><td>Disagree</td><td>ERCOT ISO supports Midwest ISO comments.

Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706.

The third bullet of the definition is largely redundant to the first two bullets and improperly references “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation.

In addition, read literally this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not “affect the electrical state or the capability of the BES”. This is not reasonable</td></tr>
</table>

Organization	Yes or No	Question 1.h. Comment (Response page 12)
		and this definition needs to be revised significantly. Furthermore, this definition does not match the current examples/criteria included in Attachment 2 that supposedly correspond to this definition. The examples in Attachment 2 appear to be arbitrary criteria that may or may not result in the system impacts included in this definition. Attachment 2 appears to be the governing document used by the SDT and this definition should be eliminated in order to eliminate technical inconsistencies and confusion.
PacifiCorp	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES Subsystems that may have a high impact in the planning time frame. The standard should address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The Medium BES Impact definition appears to mimic the definition of a Medium Violation Risk Factor. We question why there is a need to consider “planning”. Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation.
PEPCO	Disagree	The current definition for Medium BES Impact BES systems does not bring sufficient clarity for determining the appropriate category. See suggestion under High BES Impact.
NEI	Disagree	A) We do not support a review/classification of Medium BES Impact threats and therefore disagree with the inclusion of this definition. In addition, this definition could be interpreted to cover every element of the BES since it is hard to imagine how the outage of any facility would not “affect the electrical state or the capability of the BES”. B) It is recommended that Attachment 1 be used to provide an adequate definition, and that the Glossary be point to the Attachment. C) If the definition is to be kept, provide clarification for the term “directly affect”. D) Since there are BES Subsystems that do not have an impact on the BES, a “No BES Impact” should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the Appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not:

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Summary Consideration: There were many comments on the need for definitions for High, Medium and Low Impact, since these are already defined by the criteria in Appendix 1. The SDT reviewed them and has removed these definitions.

Many also commented on the absence of a "No Impact" category. It is the SDT's opinion that the definition of BES Cyber Systems effectively removes Cyber Systems with no impact from the scope, and that a BES Cyber System has some level of impact, by definition.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
Progress Energy	Disagree	Either change to No Impact (and only classify High and Medium BES Impact) or remove all bullets under Low BES Impact and add "…could not: • Directly and immediately cause or create: - BES instability; and/or - violation of an IROL • Directly affect the ability to effectively monitor and control the BES."
Dynegy	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a "Low BES Impact (Reliability)" and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with "Low BES Impact" criteria and then add a "No BES Impact" category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for "Low BES Impact" BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
GSOC/OPC	Disagree	We suggest replacing this definition with something consistent with Attachment 1.
Hayden	Agree	
SDGE	Disagree	Are the bullet items OR (mutually exclusive) or AND? Same comment applies on the need for clarity and definition of "directly affect the electrical state or capability of the BES". What does "unacceptable risk" mean, when does it become "acceptable risk"? We propose eliminating the phrase "directly affects the electrical state" – it is ambiguous and includes virtually every scenario. If "BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not: • directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures, etc." We propose this classification be changed to "No BES impact" instead of "Low BE impact".
APPA	Disagree	APPA Task Force Suggested Definition: Low BES Impact: BES Cyber Systems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, are unlikely to cause a post-contingency system state that will result in an Adverse Reliability Impact to the BES, but is still considered necessary for the reliable functioning of the BES.
Consumers	Disagree	As proposed, this lumps all other BES Subsystems into Low Impact, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule or non-existent its potential impact. What benefit is derived from identifying and placing thousands of devices in a listing of low impact? In addition, if NERC later decides that there is even one requirement in the low impact category, the compliance evidence burden placed on REs will be extremely onerous. As such, the majority of a RE's compliance tracking and evidence gathering efforts would be spent on the low impact category and critical systems will simply be part of the mix, but not receive the attention due. As mentioned earlier, this should simply be renamed as No Impact and although a listing of the subsystems may be warranted, no listing of corresponding cyber systems is justified nor should be required for this category.
NPCC	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition.
SWPA	Disagree	The definitions for High, Medium, and Low impact should not be approved for inclusion in the NERC Glossary where there may be unintended consequences for application to non-CIP standards. If the definitions are included at all, they should preface the corollary section of Attachment 1 criteria as the SDT has stated numerous times that the intent is for the definitions to be "merely guidelines" and that the criteria in Attachment 1 are the enforceable portion of the standard. Additionally, if the definitions are adopted into the standard, they should not consider the "planning time frame" which seems to be a carryover from transmission planning rather than the operational impacts of cyber assets themselves.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		Finally, the word “hinder”, which is ambiguous and subjective, should be changed to “prevent”.
MPPA	Disagree	This should have a similar quantifying reference as the first two. It recommended that the “, not categorized as High or Medium BES Impact,” be inserted into the first line such that it reads as follows: “…BES Subsystems, not categorized as High or Medium BES Impact, have Low BES Impact if…”
Central Lincoln	Disagree	No distinction is made between systems that have low impact and between systems that have no impact. While systems that have no impact should not have been included in the BES in the first place, the uncertainty around the BES definition has caused registered entities and regional entities to include such systems in the BES. This could potentially force entities unnecessarily into compliance with CIP-003 through 009. On the second bullet: Restoration from what condition? If left to overreaching regional entities, any system that could delay restoration following a small local outage will put that system in the high BES impact category even if it is not part of the BES.
NERC	Disagree	Definitions of High, Medium, and Low BES Impact each include ambiguous terms such as “contribute to”, and “create an unacceptable risk”. More specificity is required to avoid the endless interpretations of these terms and potential for inconsistent categorization of subsystems
Dominion	Disagree	See comment to 1.h. above.
Encari	Agree	
US ACE – NW	Agree	
SCE	Disagree	SCE believes that the current definition for low impact BES systems does not bring sufficient clarity to the classification process. SCE urges the Drafting Team to distinguish between those systems having a low impact and those having no impact. SCE recommends creating a “Not Applicable” category for assets that may reside in an Electronic or Physical Security Perimeter, but which have no impact on the BES. SCE also requests clarification on certain ambiguous terms. For example, the term “hinder” is ambiguous and overly broad, as it is not defined by any reference to a duration or degree of impact. The term “unacceptable risk” is also ambiguous, as it is unclear which party’s assessment of risk will be respected. It is unclear what the meaning of “electrical state” is, as that term is not defined in the NERC Glossary of terms.
USBR	Disagree	The term is defined as having no impact yet the term is called "Low Impact". The definition is not needed as there is no impact to the BES. The term can be eliminated without loss to the standard.
Dyonyx	Disagree	The term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
FMPP	Agree	
MISO	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a "Low BES Impact (Reliability)" and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with "Low BES Impact" criteria and then add a "No BES Impact" category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for "Low BES Impact" BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.
Westar	Disagree	There should be a No Impact category instead of a Low BES Impact category. Entities would then identify High and Medium Impact assets which would then require a certain set of controls. All other assets would be in the No Impact category and no controls would be necessary.
Green Country	Disagree	A single event that will not cause an Adverse Reliability Impact to the BES
Oregon PUC	Disagree	Having three impact levels is too complex and confusing for utilities and operators. We further do not see the benefit-cost need for this lower level. Also, it is difficult to prove a negative outcome as indicated by the term "they could not". We recommend there only be two BES impact levels at most. To have three levels will only cause unnecessary confusion to the industry and introduce greater opportunity for different interpretations by responsible and enforcing entities.
Manitoba 1	Agree	You probably have to also define what they could do (only defined could not). Need clarification on what is needed by third party review to make acceptable.
Portland GE	Disagree	It is unclear how an entity would be able to "prove the negative" in order to demonstrate that a BES subsystem "could not" affect the BES in the manner described in the proposed definition. In addition, it is not clear whether this requirement/definition or the requirements in Attachment 1 are the governing provisions.
PSEG	Disagree	Comment #1: Ultimately we do not believe that there is a need for a definition of "Low BES Impact" nor for a classification of Transmission Subsystem that would fall into this category. We believe that entities should only have to identify facilities that qualify as "High BES Impact" or "Medium BES Impact" and therefore have to comply with CIP-003 – 009 reliability standards. As the definition for "Low BES Impact" explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. As NERC looks towards Results-base requirements, nothing would be gained by requiring entities to list subsystems that fall under this category. We do not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		subsystem that does not fall into the “High” or “Medium” buckets will by default fall into the “Low” bucket. Comment #2: Does the phrase “hinder restoration” refer to a time delay for restoration? In other words an entity can restore their system but the cyber attack may cause some time delay for the restoration effort to be completed. Comment #3: We believe that if the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the qualifiers to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES? - Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
WE-Energies	Disagree	Wisconsin Electric Power Company agrees with EEI’s comments regarding this definition. In addition, Wisconsin Electric Power Company feels low impact subsystems should not be considered in this standard. This category includes systems that would have zero risk to the BES and as currently defined would create a large work effort to categorize and maintain with little value eliminating risk to the BES.
Idaho Power	Agree	
SOCO	Disagree	There may not be a need for the new definitions. In Attachment 1, it clearly defines the bright lines for the generation subsystems, transmission subsystems, etc. Why not just use the Attachment to clearly specify the cutoff points of each and let those be the definitions and not have them up front at all. The standard currently has criteria for High and Medium impacts and lumps all other BES Subsystems into Low, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule its potential impact. If there is even one requirement in the low impact category and that category is auditable and enforceable, the compliance evidence burden placed on entities will be onerous. Since there is no bottom to this standard and low is the ‘everything else’ category, every cyber system in the BES of North America will be on the list and in scope. There may be tens of thousands of systems per entity (would not each relay be a ‘cyber system’?). The majority of your compliance tracking and evidence gathering will be on the lowest impact, but orders of magnitude more numerous cyber systems. If the TFE process also applies to these millions of systems continent-wide we are creating an unmanageable bureaucracy. The standard needs minimum criteria. Since the Low impact category is simply a catchall, we propose there be no requirements for low. This definition is covered in Attachment 1 with greater detail, thus drop this definition in lieu of the Attachment 1 definitions. General section comment: Insert a diagram to clarify the delineation of the defined terms as related to each other.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
DTE	Disagree	The intention of this category seems to be to capture all BES subsystems that are not High or Medium BES Impact. Changing the language from a qualifier to a disqualifier could cause confusion. To keep the language in parallel with High and Medium BES Impact, we suggest changing the definition as follows: Low BES Impact — BES Subsystems not classified as High BES Impact or Medium BES Impact. If the drafting team does not agree with our version of the definition, we are concerned that the term “unacceptable risk” is reintroducing the “acceptance of risk” concept that was removed from previous versions.
AEP	Disagree	Since there are BES Subsystems that do not have an impact on the BES, a “No BES Impact” should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the appendix). While the current “one size fits all” approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.
Edison Mission	Disagree	The term “unacceptable risk” is an inappropriate term for this portion of the standard. Considerable discussion has been made and confirmed that CIP-002 / R1 is an “impact” analysis and does not consider risk. This is a 180 degree turn from the original intent of the standard and will cause considerable confusion in applying the provisions of the standard if the term “risk” is allowed to remain in the definition.
Calpine	Disagree	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	Disagree	The criteria for "low" impact seems to us to represent *no* impact, which we presume is not the SDT's intention. We recommend this definition be revisited.
Flathead	Disagree	Low impact assets by definition are not critical. It defies logic that they would be included as critical and subject to CIP-003 through CIP-009 just like the actually critical assets.
E ON	Disagree	E ON U.S. sees no need for this category. Inclusion of this category establishes the necessity of inventorying and assessing the BES impact of every conceivable BES Subsystem. Given that by definition BES subsystems falling into

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		this category have no impact on overall BES reliability, E ON U.S. questions the need for such an expansive exercise and use of limited resources
Carthage	Agree	
WECC	Disagree	If this is could not impact then this should be “no impact” not low impact.
Entergy	Disagree	Has little practical relevance in the matter of mitigation of vulnerabilities and/or threats to cyber security of control systems; may have relevance in the area of physical security of grid assets/facilities, but not cyber security.
CenterPoint	Disagree	Disagree – See comments on 1.a and 1.h. This appears to be a definition of “no BES impact” and therefore should not be listed as “Low BES impact”. BES systems that do “not” cause any of the impacts listed should not require security measures to be employed.
LCRA	Agree	1. The “Low BES Impact” category must result in very few security controls. 2. The phrase “directly affect” should be changed to “directly and adversely affect”. The original phrase is too broad.
FRCC	Disagree	See comments to question 1.h
NIPSCO	Disagree	We do not believe that there is a need for a definition of “Low BES Impact”. As the definition for “Low BES Impact” explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. Suggestion: Eliminate the proposed category or review and revise the criteria of a Low BES impact asset.
ConEd	Agree	
EEI	Disagree	EEI believes that the current written definition for low impact BES systems does not bring sufficient clarity for determining the appropriate category. Use of phrase: “BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not:…” creates a nearly impossible burden of proof. It is difficult or impossible to ‘prove’ or demonstrate a system has these properties. Moreover, terms such as ‘hinder’ are vague and open to wide interpretation. In addition, the state of the electrical system is affected “directly” by normal events, such as customer load. Finally, we do not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any subsystem that does not fall into the “High” or “Medium” buckets will by default fall into the “Low” bucket.
O&R	Agree	
Alliant	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of Medium BES Impact is actually set by DPI-002 - Attachment 1.
Ameren	Disagree	We disagree with what is considered "Low BES Impact". If it is necessary that all BES Subsystems need to be in one of the three categories then Low BES impact should be defined as all BES Subsystems that are not included in High BES

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		Impact or Medium BES Impact. However, we believe a fourth category should be added which is “No BES Impact”, for example radial facilities. If this suggestion is adopted then the Low BES Impact offered should be revised accordingly, e.g. loss of load less than 100 MW.
Black Hills	Disagree	What proof is necessary to justify a "could not" declaration? Other common term questions as in previous sections.
TNMP	Disagree	Comments on High BES Impact are equally applicable to this definition.
NVEnergy	Disagree	We understand the concept behind this definition, but note that as written, it carries the same degree of vagueness that we object to in the High and Medium categories. Also, we wish to note that if the above bullets are true (no unacceptable risk to BES, no hindrance of restoration, no effect on capability nor ability to monitor the BES), then it is unreasonable to assign even a “Low Impact” to the subsystems. Perhaps a “No Impact” category is in order.
MWDSC	Disagree	Unclear whether "BES" is referring to an isolated unavailable system or an interconnected system. Recommend adding a bullet to the term "Low BES Impact" such as…. "..not: create an Adverse Reliability Impact (as defined in NERC Glossary) of any interconnected BES". Also, if an engineering evaluation demonstrates no Adverse Reliability Impact of any interconnected BES, recommend adding a separate category such as "No BES Impact" or a subcategory under "Low BES Impact" with limited application of unknown security requirements in CIP-003 through CIP-009.
Empire	Disagree	Optional Definition: A single event that will not cause an Adverse Reliability Impact to the BES.
NCEMCS	Agree	
BCTC	Disagree	See Question 13
SWTC	Disagree	Until the BES Definition is resolved, how can an entity do an impact analysis.
SCEG	Agree	
Exelon	Disagree	Exelon is concerned that with the High, Medium and Low BES Impact definitions combined with the Attachment 1 Criteria would result in confusion and an inconsistent approach with respect to other NERC Standards. Exelon therefore suggest that the SDT adopt the following approach: Eliminate the High BES Impact, Medium BES Impact, and Low BES Impact definitions. Establish a single formal definition for “BES Impact” such as “BES subsystems that if destroyed, degraded, or otherwise rendered unavailable directly impact the function of the BES. Categorization of impact is determined based on guidelines provided in Attachment 1 of this Standard.” Refer entities to Attachment 1 for categorization of elements (high/medium/low), with the assumption that SDT will provide clearly defined criteria for BES impact categorization.
BPA Trans	Disagree	Some of our comments for High BES Impact are applicable and are repeated here: 1. The way the identification of Impact levels is defined, it appears no BES Subsystem or "supporting" cyber system will

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		be off the list. The differentiation will be in the impact levels assigned. From a pure cyber security perspective this makes sense, but: "BES Cyber Systems need to be “secure” not for the sake of being secure; but to provide assurance (i.e., grounds for confidence) in the resiliency of these functions". (from the December 2009 Draft Guidance document Page 3 "purpose of categorizing BES Cyber Systems".) From a practical perspective, compliance might prove to be problematic because of the way the impact levels are designed to be assigned/implemented. If the Identified BES Subsystem is rated as a High Impact subsystem, then any supporting Cyber Systems are required be rated High impact, regardless of their real impact. See the table Draft (CIP-00204 Attachment 1) for categorization criteria. This is an incorrect assumption. It is possible to have cyber systems that support BES subsystems, which, if lost, degraded or compromised, will have no significant impact (or no impact) in the function, operation or security of the BES subsystem. The security risk level of a cyber system should be rated on its potential effect on the BES Subsystem it supports, not on the rating of the supported BES Subsystem. 2. The definition depends too much on other undefined, vague, or ambiguous terms, such as "planning time frame", “unacceptable risk,” “hinder restoration,” etc. In particular, what is, and how long is a "planning time frame"? 3. The structure of this impact statement is confusing. It appears that the bullet items apply only when the Subsystem is “destroyed, degraded or otherwise rendered unavailable.” But, each bullet item refers to what the Subsystems could do under those circumstances. This is unclear, since the Subsystem can do nothing if it is destroyed or rendered unavailable. It would be much clearer to talk in terms of “Subsystems whose destruction, degradation, or lack of availability could lead to …” The FIPS-199 approach, in terms of the severity of impact on operations, assets, or individuals may be useful. Additionally, 4. It appears that this definition is too vague. Recommend the last two bullets read "directly and adversely affect…" Any adverse affect, no matter how small, would cause the Subsystem to have at least a Medium Impact. This is really a definition of "No Impact", not "Low Impact". 5. Bullet 2 should read: "directly hinder restoration of the BES to a normal condition." "Directly" is needed in this instance to make it clear that indirect affects are outside the scope of the definition. "Of the BES" is again needed so we know what the reference is. 6. Are these four bullets joined by "and" or "or"? The intent would seem to be "and": if the Subsystem could do any one of the things listed in the bullets, it could not be Low impact. However, since the conjunction is not specified, one could argue that a system that could do 3 of the 4 could still be Low Impact. Again, the FIPS-199 approach could be useful. It limits "Low Impact" to systems that would have a "limited adverse effect". This is much more realistic. Note also that FIPS-199 ignores systems that can have no effect. This is appropriate.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		We suggest that the 3 tiers of impact be High, Moderate and Low Impact/Not Applicable.
HQT	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
CCG	Disagree	CCG does not support the definition of "Low BES Impact" nor the concept of categorizing all assets into three groups, all of which will require some level of protection. Categorizing BES assets as "Low Impact" when the definition specifically states these assets "could not" have any impact is entirely inappropriate. This exceeds what is needed for reliability.
Allegheny Energy	Agree	
KCPL	Disagree	If this is the direction the CIP Standards Drafting Team believes this Standard should go, much more clarity and guidance will be required to establish practical criteria for combinations of generation and transmission loss or misuse to consider.
Connectiv Energy	Disagree	See comments for 1.g above.
MidAmerican	Disagree	Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition is not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset.
CPG	Disagree	This definition should just state that it includes all other BES Subsystems not defined as High or Medium BES Impact. Since this group of subsystems does not fall into the High or Medium Impact levels, the name of this group should be changed to "No BES Impact."
Santee Cooper	Disagree	See comment to Medium BES Impact.
OGE	Disagree	• The terminology is too vague. What is "an unacceptable risk"? How much of an impact must occur before something has "directly affected" the BES? • "Normal condition" needs to be defined in this context. • OPTION: A single event that will not cause an Adverse Reliability Impact to the BES. A post contingency system state that will not cause an Adverse Reliability Impact to the BES.
Oncor	Disagree	The enforceable definition of Low BES Impact is actually set by CIP-002 - Attachment 1. The descriptions of what "Low BES Impact" is not should be included in Attachment 1.
PPL Supply	Disagree	Comments: Agree with EEI Comments.
St. George	Disagree	As a small municipality, we applaud the draft team for dealing with the over-simplistic classification of an asset as Critical or Non-Critical. The proposed standard takes two classifications (Critical and Non-Critical) and makes three (High, Medium, and Low). We are deeply concerned that three classifications are not sufficient to represent the true nature of the BES. At minimum another classification should be added: Minimal. This would be for Generation Subsystems below 200 MVA and transmission below 150 kV in the Eastern and Western Interconnections. Low would then be for Generation Subsystems of 200 – 1,000 MVA and transmission of 150 – 200 kV in the Eastern and Western

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		Interconnections. The Minimal classification assets would then be exempt from CIP-003 through CIP-009 in the same way Non-Critical assets are currently.
NGRID	Disagree	It is still unclear if "low BES Impact" systems will require any security controls and will be clear only when CIP-03 through CIP-09 are released. If they do not require any security controls (which currently looks to be the case), it is recommended to delete this definition. Nothing will be gained by maintaining this list especially as we move towards Results based Standards. If the SDT wants to keep this definition that they need to provide more clarity as to what BES Cyber Systems will be included in this category. - What are the parameters to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES?
MGE	Disagree	Recommend that this section be completely removed. CIP-002-Attachment 1 actually defines High, Medium, and Low BES Impacts, this will only lead to confusion since it is not a mirror image of CIP-002-Attachment 1. MGE does not support the three level approach. MGE would support a four level approach that has the addition of a "No BES Impact" category. This category would contain cyber assets contained in a Registered Entity's UFLS program. The purpose of the UFLS program is to provide a last resort for system preservation. It is not defined in the UFLS Standards that the UFLS program is to maintain BES stability, but that is why there is a UFLS program. By not having a No BES Impact category, the SDT is not giving a bright-line solution for those entities who are only DP's with an UFLS program, etc. When given a Bright-line solution, the entity will see that that there are two sides. The three category has all cyber assets on one side. The No Bes Impact category will give the SDT and the entire industry the solution to this issue by stating what cyber assets impact the BES and which don't (No BES Impact).
FE	Disagree	We do not support a review/classification of Low BES Impact threats and therefore disagree with the inclusion of this definition. If it remains, then Low BES Impact Subsystems should require minimal or no security controls since by definition the Low BES Impact would NOT contribute to BES problems.
TECO	Disagree	We support EEI's comments and offer the following additional suggestions. The term "unacceptable risk" needs to be more clearly defined. Additionally we are concerned with the existence of VSLs that relate to subsystems that by definition have no impact.
CECD	Disagree	If a BES Subsystem cannot directly affect the electrical state or capability of the BES or directly affect the ability to effectively monitor and control the BES the Registered Entity should be able to state that there is No BES Impact.
MRO	Disagree	The definition should be completely removed from the Definition of Terms section because the enforceable definition of High BES Impact is actually set by CIP-002 - Attachment 1.
GTC	Disagree	We suggest replacing this definition with something consistent with Attachment 1.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
Xcel	Disagree	See 1.h. In general, we believe the Attachment defines Low, Medium and High and these should be removed from the reference section.
BGE	Disagree	We believe that the definition of “subsystem” is unclear and needs further clarification. It needs to be more explicit. The word “destroyed” is inconsistent with prior definitions. Items 1 d, 1 e, 1 g, 1 h should use the same terminology. We suggest the phrase “loss, degraded, or rendered unavailable” be used. 1st bullet….”unacceptable risk” not well defined. It is vague and should be linked to NERC transmission planning standards. “Cascading Sequence of failures” is not clearly defined We feel that the bullet, “directly affect the electrical state or the capability of the BES;” should be removed. The statement is too broad. In the phrase, “Or could hinder restoration to normal condition”, “normal condition” is not clearly defined. Also, please note response to Q3. We believe that there should be a “No Impact” category. This could be accomplished by eliminating the “Medium Impact” category and redefining “Low Impact” with the current “Medium Impact” definition as modified with our comments in 1.i.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although we appreciate the idea of categorizing an impact as low, we do not think it provides any additional benefit to the BES since most of the key points have been captured in the high and medium.
TAPS	Disagree	The proposed “low impact” category, as currently defined, includes subsystems--and, therefore, cyber systems--that have no impact on the bulk electric system. Cyber systems that have no potential impact on the reliability of the BES should not be subject to security controls. Nor should such systems be subject to NERC's registration and compliance regimen. By capturing such facilities, therefore, the proposed standard would impose significant costs on responsible entities and Regional Entities with no commensurate benefit to reliability. The lack of impact on the BES also puts the statutory basis for such coverage into question. To achieve the standard’s cyber security purposes in a cost effective and rational manner, consistent with Section 215, the identification of cyber assets should be restricted to those facilities that have a meaningful potential impact on the BES; cyber assets with no potential impact on reliability should be classified in a fourth, “No Impact” tier. This approach is consistent with the statement of Gerry Cauley in his planned comments to the MRC on Monday, February 15 (available at http://www.nerc.com/docs/mrc/agenda_items/AgendaItem_6.pdf) that there should be “minimum bright-line criteria for identification of critical bulk power system assets.” The existence of a “bright line” necessarily entails the exclusion of systems, such as those with no impact on the BES, that fall below the “bright line.”
Allegheny Power	Disagree	AP believes that the current written definition for low impact BES systems does not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Attachment 1 to make such determinations.

Organization	Yes or No	Question 1.i. Comment (Response page 13)
FMPA	Disagree	See comments to Medium BES Impact concerning ambiguous definition FMPA suggests a less ambiguous definition of: “BES Cyber Systems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, are unlikely to cause a post-contingency system state that will result in an Adverse Reliability Impact to the BES, but is still considered important to the reliable functioning of the BES.” Or possibly more clarity by specifying "more than a single contingency away" from an Adverse Reliability Impact. Also, it is difficult to develop an opinion on Low BES Impact without understanding what requirements, if any, will be imposed on Cyber Systems with Low BES Impact in standards CIP-003 through CIP-009. We cannot agree with the definition until these requirements, if any, are made clear. We believe strongly that there is no need to regulate cyber security of Low BES Impact Cyber Systems, and any requirements placed on Low BES Impact Cyber Systems would be against the intent of the EPAct of 2005, which was specifically geared towards maintaining “reliable operations” to prevent “instability, uncontrolled separation, or cascading”, which is already captured in High BES Impact. If the SDT believes that some requirements are necessary for the Low BES Impact Cyber Systems, such requirements should be programmatic in nature and not Cyber System specific, such as training. Any Cyber System specific requirements for Low BES Impact Cyber Systems would be unduly burdensome to the Entities with no value to BES reliability.
Duke	Disagree	This definition is not needed because Attachment 1 of the standard clearly explains that all BES Subsystems which are not High BES Impact or Medium BES Impact are Low BES Impact.
NBSO	Disagree	This definition is not clear and has conflicts with Attachment 1. Recommend removing this definition
AESI	Disagree	We suggest replacing this definition with something consistent with Attachment 1.
IESO	Agree	The term "risk" is misused in the phrase "unacceptable risk of". the term should refer to the "unacceptable likelihood of" Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we’ve got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): a. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. b. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined according to studies or other criteria determined by the RC. c. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring compliance.
Manitoba 2	Disagree	The definition “Low BES Impact” should be considered a definition applicable only to the CIP Cyber Security Standards, and not be added to the general NERC Glossary of Terms, due to potential unintended consequences of applying this

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		definition to the entire body of NERC Reliability Standards. It may not be necessary to create BES Impact definitions, as the impact criteria contained in CIP-002 - Attachment 1 Criteria for BES Impact Categorization of BES Subsystems already define High, Medium and Low BES Impacts. By the definition, these BES Subsystems do not have an impact on the reliability of the BES, and therefore should belong in a “No BES Impact” category. If a “No BES Impact” category is not provided, the controls for the Low BES Impact category should not be auditable. There needs to be some consideration of acceptance of risk for minimal reliability benefit. A categorization level where no mandated security controls are required should be included. Previous comments regarding a “No Impact” category by multiple entities responding to the concept paper, including Manitoba Hydro, were not incorporated into this latest version of CIP-002. Agreement with these definitions is not possible without the associated security measures and implementation plan, which have not been provided at this time.
OMPA		OMPA suggests the addition of an additional tier for “no BES impact”.
ATC	Disagree	Ultimately ATC does not believe that there is a need for a definition of “Low BES Impact” nor for a classification of Transmission Subsystem that would fall into this category. We believe that entities should only have to identify facilities that qualify as “High BES Impact” or “Medium BES Impact” and therefore have to comply with CIP-003 – 009 reliability standards. As the definition for “Low BES Impact” explains, subsystems that fall under this category could not impact (result in cascading, instability or separation) the BES. As NERC looks towards Results-base requirements would is being gained by requiring entities to list subsystems that fall under this category. If the SDT rejects our above recommendation: 1. ATC does not believe that this level needs to have a specific definition because it is a catch all bucket for subsystems. Any subsystem that does not fall into the “High” or “Medium” buckets will by default fall into the “Low” bucket. If the SDT does not agree with our suggestion to delete this definition then we believe that they need to address the following questions: 2. Does the phrase “hinder restoration” refer to a time delay for restoration? In other words an entity can restore their system but the cyber attack may cause some time delay for the restoration effort. (The delay will result in X amount of hours over planned activities) Lastly ATC believe 2. If the SDT wants to keep this definition then they need to provide more clarity as to what BES Cyber Systems will be

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.i. Comment (Response page 13)</th></tr>
<tr><td></td><td></td><td>included in this category.
- What are the qualifiers to determine if a BES Cyber System could not directly affect the electrical state or capability of the BES?
- Does effectively monitor and control mean a two part qualifier. (The impact has to not only interrupt the data coming to you by also has to hinder your ability to control the system? If you can control the system trough a manual process would this then not qualify under medium?)
(Please see our comment to question 1e)</td></tr>
<tr><td>LES</td><td>Agree</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:
(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable -</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 1.i. Comment (Response page 13)</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Private</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>It appears this is the catch all bucket for all remaining BES Subsystems. It is unclear whether an entity would be required to prove that a BES Subsystem "could not" do as bulleted which seems of little value. It is unclear why every BES Subsystem must be categorized at all instead of focusing purely on that which is "high" and "medium". The subsequent need (R1) to update and maintain lists as a result of this is labor intensive and because CIP-003 through CIP-009 modifications for version 4 have not been provided it is difficult to determine the value in this exercise.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>The Standard and Attachment 1 both define what constitutes a Low BES Impact. IMPA recommends deleting this definition and following Attachment 1 criteria when it comes to determining what is a Low BES Impact.</td></tr>
<tr><td>ERCOT</td><td>Disagree</td><td>ERCOT ISO supports Midwest ISO comments.

Midwest ISO Comments: In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706.

Furthermore, this definition is inherently inconsistent. It essentially states that all remaining BES Subsystems have a “Low BES Impact (Reliability)” and their associated BES Cyber Systems require protection when the stated definition does not identify any reliability impact. This definition needs to be modified to reference a new Attachment 3 with “Low BES Impact” criteria and then add a “No BES Impact” category. If this is not done, the protection measures to be included in CIP-003- CIP-009 for “Low BES Impact” BES Cyber Systems must be either none or minimal since there has been no identified reliability impact identified for these BES Subsystems.</td></tr>
<tr><td>PacifiCorp</td><td>Disagree</td><td>- Criteria such as Attachment 1 (or other bright line criteria) achieve the needed objective. This definition in not needed and does not bring sufficient clarity in determining security controls categorization. Impact categories are better defined by considering the span of control of the Cyber Asset. If the definition is needed, it should not include any reference to BES Subsystems that may have a high impact in the planning time frame. The standard should</td></tr>
</table>

Organization	Yes or No	Question 1.i. Comment (Response page 13)
		address BES Subsystems according to their current rating and impact, not a potential future rating or impact.
IRC	Disagree	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. The Low BES Impact definition appears to mimic the definition of a Low Violation Risk Factor. We question why there is a need to consider "planning". Planning in the VRFs refers to transmission planning. CIP standards should consider the operational impacts of cyber assets only. The only planning involved for cyber systems should be how to plan to make existing cyber systems comply with the standards and how to make new systems compliant upon installation
PEPCO	Disagree	The current definition for Low BES Impact does not bring sufficient clarity for determining the appropriate category. Use of phrase: BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not… creates a nearly impossible burden of proof. It is difficult or impossible to prove or demonstrate a system has these properties. Moreover, terms such as hinder are vague and open to wide interpretation. In addition, the state of the electrical system is affected directly by normal events, such as customer demand. See suggestion under High BES Impact.
NEI	Disagree	A) NEI does not support a review/classification of Low BES Impact threats and therefore disagree with the inclusion of this definition. If it remains, then Low BES Impact Subsystems should require minimal or no security controls since by definition the Low BES Impact would NOT contribute to BES problems. B) Since there are BES Subsystems that do not have an impact on the BES, a "No BES Impact" should be added to the existing High, Medium, and Low impacts. Also, there is a clear need to approach these impacts by function (a good starting list is developed in the Appendix). While the current "one size fits all" approach has simplicity appeal, it can not effectively capture the detail necessary to address the technical considerations present in each of the functional areas.

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: There were a number of comments related to the absence of consideration for how BES cyber systems are connected in the categorization process. After much discussion, the SDT agrees that network connectivity should be a consideration, but that it is more appropriate to be considered in the drafting of requirements or controls that apply to categorized BES Cyber Systems or their components.

There were comments that addressed the approach where inheritance from the BES Subsystem Impact level would result on the same level of impact for all BES Cyber Systems associated with the subsystem. The SDT has made substantial changes to the draft to allow entities to use any method to identify BES Cyber Systems (i.e. to start with an inventory of all BES Cyber Systems, or to start with BES Facilities and the BES Cyber Systems supporting their real-time operations), as long as all BES Cyber Systems are identified.

Many respondents noted in their comments that they can only evaluate the purpose if the requirements and controls are posted together. The SDT has considered these comments and is posting the new draft together with drafts of the requirements or controls.

The Purpose has been redrafted to reflect these considerations. The new purpose (CIP-010-1) is:

Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.

Organization	Yes or No	Question 2 Comment (Response page 14)
Progress Energy	Disagree	To provide additional clarity, CIP standards should only address real-time cyber operations. See also the Question 1 comments above.
Dynegy	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems as critical and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets

Organization	Yes or No	Question 2 Comment (Response page 14)
GSOC/OPC	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Hayden	Disagree	CIP-002-4 overly complicates the approach delineated in CIP-002 (earlier versions). In the earlier versions it was a straightforward approach where the Registered Entity identified its Critical Assets (i.e., those assets that could affect the BES) and then you identified the supporting Cyber Assets and then the Critical Cyber Assets. The approach in this newly revised standard takes this systematic approach and appears to complicate the process with new terms and definitions that I am not certain help the Registered Entity better understand the process. Attachment 1 is helpful in providing more specifics on what constitutes a Critical Asset so why not just use Attachment 1 to say that if you have an asset and it satisfies these requirements it is now a Critical Asset?
SDGE	Disagree	We agree in principle with the purpose statement, but in several locations throughout the Standard the drafting team uses ambiguous language that needs to be easier to understand and interpret. Examples include: • Identifying BES Cyber Systems is plausible, given the language in this draft. However, the categorization of BES Systems given the existing language is likely to result in multiple interpretations and inconsistencies throughout the industry. • Because the “High BES impact” and “Medium BES impact” definitions are so close to each other, security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES could require entities to implement the same or very similar controls for the “High” and “Medium” impact classes to ensure compliance. • How will certain CIP-003 through CIP-009 requirements be treated for the three BES impact classes such as training, vulnerability assessments, PRAs, access controls, etc.? Again, we propose having just two impact classes to help make the implementation and management of these Standards easier.
APPA	Disagree	APPA Task Force Comments: The addition of new terms of "subsystem" and "functions" add complexity and confusion. How are these new functions related to the Functional Model, for instance? The real focus ought to be on the worst case contingencies / scenarios that can be caused by malicious manipulation of a cyber system. Such a focus bypasses the need to create new terms such

Organization	Yes or No	Question 2 Comment (Response page 14)
		as subsystems and functions.
Consumers	Disagree	We do not believe the proposal accomplishes the goal because the cyber systems simply inherit the categorization of the BES Subsystem. To apply appropriate cyber security controls, the SDT needs to create a means so that cyber systems are categorized separately from the subsystems. As in previous versions of the standard, first address the critical nature of the subsystems (assets) then address how critical (or not) are the associated cyber systems. The requirements for protecting these assets (via CIP-003 >> CIP-009) should then vary based on how critical the cyber system is to the functioning of the subsystem. Note that this means that ALL cyber systems would not need to be categorized, but only those that are associated with the critical BES Subsystems. Much like the previous revisions of CIP-002, a “critical” evaluation/test needs to first be passed before further investigating the cyber assets. The exception would be those systems (subsystems according to the new definition), such as SCADA, but only if that (or similar systems) have external routable protocol, networking, or dial-up connectivity. If FERC wants to issue one order to include all CIP Version 4 standards, they should hold the vote on CIP-002-4 through CIP-009-4 at the same time after review and comments have been made on all eight standards. The industry should have an understanding of all the CIP version 4 standards before voting.
NPCC	Agree	
SWPA	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on “functions critical to the reliable operation of the Bulk Electric System (BES)”. Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems and to require protection. The drafting team should establish bright lines for criteria which could satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.
MPPA	Disagree	The standard, in its current form, does not accomplish its purpose. The standard needs to quantify the differences of High, Medium, and Low BES Impact definitions in a clearer manner. It needs to provide consistency between the R1 VSL, and the R2 VSL.
Central Lincoln	Disagree	See 1.i. above.
NERC	Disagree	The standard appears to draw an implied distinction in the purpose statement and in the definition of BES Cyber System by using the language about functions “critical to the reliable operation of the BES”. While Attachment 2 defines the eight BES critical functions, we create an unneeded distinction by using the word “critical”. Critical is not defined nor is an understood framework available for use. The team can achieve the same goal by changing the purpose statement and Attachment 2 to eliminate the use of “critical” and replace it with “necessary”, a word that is straight forward in its definition and that does not carry the existing concerns.
Dominion	Disagree	CIP-002-4 does not accomplish the objective because of the uncertainty it introduces. Clear, concise and well-defined

Organization	Yes or No	Question 2 Comment (Response page 14)
		statements and terms are needed to satisfy the stated objective.
Encari	Agree	
US ACE – NW	Agree	
SCE	Disagree	SCE recommends that the Standards Drafting Team put forward a single package of proposed standards that includes both the proposed standards for BES Cyber System Categorization, as well as the associated control standards. This would allow the industry to perform an overall impact analysis of the proposed standards and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of the associated controls in CIP-003 through CIP-009. SCE's recommendation is based on the fact that it is impossible to judge the proposed purpose behind CIP-002-4 without considering the types of controls that will follow from categorizing BES Cyber Systems as "low, medium or high" impact systems. The nature of controls will vary vastly between what is high impact electrical and cyber versus simply high impact electrical, and the industry is not in a position to make any judgments about this stated purpose until it sees the type of controls that NERC proposes will support that purpose. Finally, SCE is concerned by the fact that the proposed three levels of categorization for the BES Cyber Systems ignore the great importance of cyber connectivity. For example, an IP routable network type of cyber system will have a different set of vulnerabilities than one that is based on dial-up connectivity. These two channels of electronic access will differ from a network based on serial protocols. This is concerning to SCE because the technical architecture of a particular network type and the data being communicated on it is amenable only to a select set of security controls. While some security controls are universally applicable they may not offer targeted protection to control systems in a manner where the control is commensurate with the vulnerability.
USBR	Disagree	It is not clear what added value is achieved by categorizing assets or cyber systems other than having an impact. FERC has clearly stated no risk is acceptable. Grading the assets asserts a level of risk. The proposed standard should describe objectives of criteria which the Responsible Entities need to develop to assess BES impacts for either Assets or Cyber Systems. The proposed standard does appear to describe requirements of when the criteria is to be used, which is good. Unfortunately the "criteria" tries to identify elements rather then what the Responsible entity should use to assess the elements. As indicated in the comments and suggested changes for the other sections, the language needs to be clarified.
Dyonyx	Agree	
MISO	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems as critical and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.

Organization	Yes or No	Question 2 Comment (Response page 14)
Westar	Disagree	Again, there is a large number of BES assets that have absolutely no Adverse Impact on the BES. There needs to be a No Impact category.
Green Country	Disagree	It clearly is not commensurate since in the situation of NO impact to the BES, the next step the asset up to LOW impact and will require compliance with CIP-003 thru 009 at some level. Which again is not following the Standard Process Manual “Market principals” bullet point #1. It gives an unfair business advantage to regulated utilities to recover costs through rate base.
Oregon PUC	Disagree	CIP-002-4 as proposed is too complex and vague for industry implementation. This is a cornerstone standard that will set the basis for other NERC and regional standards (especially CIP-003 through CIP-009). We believe that clarity, specificity, technical accuracy and relative simplicity are critical for this standard. At the very least we recommend that the Lower BES Impact level be eliminated.
NB Power Gen	Agree	In general I agree that this draft of CIP-002-4 significantly improves identifying and categorizing the BES Cyber Systems that support the functions critical to the reliable operation of the BES. However, as noted in my previous comments, the application of security controls commensurate with the impact should also include the context of threat. The current CIP-002-4 seems to me to change the context to include much more than threats from remote access. If we are protecting against the threat of single or multiple simultaneous remote access to our systems, then we should recognize that lack of the possibility of such access should be recognized as a secure state that does not require additional security measures other than appropriate change management to ensure no new access is introduced. Otherwise, the full range of CIP standards will be applicable to all cyber systems whether stand alone or not, which is perhaps more of a physical security issue (items of concern are only accessible within the facility).
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree that the proposed CIP-002-4 achieves the stated objective. Cyber systems are not identified and Attachment 1, specifically 1.10, 1.11, 1.12, would require various multiple studies of the subsystems identified because it is unclear as written how widespread an event would have to be to constitute “voltage collapse” or “system collapse." In addition, it is unclear, if the language is intended to get at a very granular level, whether the data is available. There is no way to know whether the controls are “commensurate with the potential impact” without understanding what the full extent of those controls will be for assets that are rated as High, Medium, or Low BES Impact. This standard as proposed is too vague in definition and too complex and burdensome in implementation to justify any perceived marginal enhancement to reliability that may result from the proposed changes. Clarity and specificity that can be uniformly applied across utilities and for auditors is necessary for this standard.
PSEG	Disagree	Comment #1: We believe that the purpose of this standards is to identify those BES Cyber System which are “critical” (i.e. could cause instability, separation or cascading) to the BES. Suggestion: To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) which are “critical” (i.e. could cause instability, separation or cascading) to the Bulk Electric System (BES) as a basis for applying security controls.

Organization	Yes or No	Question 2 Comment (Response page 14)
		Comment #2: We believe that the approach utilized makes an effort to categorized BES assets but does not take the same effort to categorize BES Cyber Assets. The BES Cyber Asset now inherits the impact categorization of the BES asset. This again creates a one-size fits all solution for the cyber requirements of the BES Cyber Asset. Comment #3: We believe that if BES system didn't have external connections, it should not be included as an asset to be protected.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI's comments regarding this question. We also would like to note that we disagree with the inclusion of cyber assets that utilize a non-routable protocol. These devices do not pose a threat from external attack. In addition, Wisconsin Electric Power Company feels a cyber system is one that has connectivity to a network or the Internet. Devices that may be isolated or stand-a-lone systems where there is no network connectivity should not be considered a cyber system.
Idaho Power	Disagree	The criteria to categorize the cyber systems are too vague and will not provide good guidance to the entities attempting to categorize their cyber assets. If the cyber system supports a function critical to the reliable operation of the BES, haven't you by default categorized it as critical (high). Why go through the effort to categorize the BES subsystems if the cyber systems have already been categorized as critical in Attachment 2 if they support one of the listed functions.
SOCO	Agree	The effective date of this Standard should be directly related to the effective dates of all forthcoming daughter standards. The scope of these standards are very extensive, the requirement to categorize all systems within less than 2 years and to maintain this categorization without further active standard requirements presents an unnecessary burden. Consideration should be given to the potentially limited supply of hardware and knowledgeable personnel to the electric and other critical infrastructure industries for compliance with this and other similar regulations.
DTE	Agree	
AEP	Disagree	AEP is interested in the same outcomes as though of the SDT – a secure and reliable Bulk Electric System (BES). In fact, AEP believes that the SDT is headed in the direction, but has not been given enough time to get to the necessary results. AEP is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation (http://www.nerc.com/fileUploads/File/CIP/706-SDT-Webinar-Presentation.pdf) with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low." The resulting table outlines a graduated level for applying cyber security controls to BES Cyber Systems based on risk.

Organization	Yes or No	Question 2 Comment (Response page 14)
		BES Cyber Systems that have a low risk should not require the same cyber security controls as BES Cyber Systems that pose a high risk. Ratcheting the risk level to protect nearly everything will inadvertently result in a decline in the reliability of the BES.
Edison Mission	Agree	
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	Opposed to new definitions until existing definitions are clarified sufficiently
E ON	Disagree	E ON U.S. does not agree that CIP-002-4 accomplishes the intended objective. The definitions are, as noted above, in several instances too expansive and ambiguous. Identification of BES cyber systems becomes an exercise in categorizing every cyber component associated with any operating facility of any type. Also, cyber-systems associated with marketing or other non-operational functions (e.g., planning) are specifically mentioned as being excluded from consideration in the Categorizing Cyber Systems: An Approach Based on BES Reliability Functions document (page 7) unless they also affect the reliable operation of the BES. These systems are not specifically excluded in the draft standard. E ON U.S. suggests including this specific guidance under one of the existing definitions (e.g., BES Cyber System or High/Medium BES Impact).
Carthage	Agree	
WECC	Disagree	Although NERC has taken a focus on impact based analysis, the definitions are still too open to probability and interpretation in the risk assessment with terms such as “could potentially”, “unacceptable risk”, and “hinder”. If NERC wishes the probability to be considered 100% then all ambiguity and potential for interpretation needs to be removed from definitions.
Entergy	Agree	This is the proper ‘purpose’ of the standard, but the specified required approach to reach this purpose is ill-conceived. Specific recommendations for properly addressing the issues at hand are presented in response to Question 13 below.
CenterPoint	Disagree	Disagree – Setting aside the flaws of the subsystem approach, it is not clear what will be the basis for applying security controls commensurate with potential impact. Therefore, it is not clear whether CIP-002-4 would accomplish any objective.
Ca Cogen	Disagree	As explained above, the concern is with accessibility. Security controls should be applied only to those assets that are vulnerable.
LCRA	Agree	It is very difficult to properly evaluate the revised CIP 002 document without being able to see the rest of the revised standards. While the underlying assumption for categorizing BES Cyber Systems is the need for differing levels of protection, it is unclear how the existing standards CIP 004-009 will be applied to these systems.

Organization	Yes or No	Question 2 Comment (Response page 14)
NIPSCO	Disagree	We believe that the approach utilized makes an effort to categorize BES assets but does not take the same effort to categorize BES Cyber Assets. The BES Cyber Asset now inherits the impact categorization of the BES asset. This again creates a one-size fits all solution for the cyber requirements of the BES Cyber Asset. Suggestion: Eliminate the BES protection level inheritance. Allow the cyber assets to be evaluated based on the impact to the asset, not based on the impact of the asset to the BES. If this inheritance approach was left as proposed by the SDT, we would need to see how the one size fits all approach is being addressed throughout CIP-003-4 through CIP-009-4.
ConEd	Disagree	Need improved clarity in the definition. Use examples of the common systems and show how they would be categorized. There is too much engineering analysis required to determine if a system belongs in the high or medium category.
EEI	Disagree	EEI is very appreciative of the efforts of the drafting team. In particular, we believe that it is important and appropriate to apply "security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations.
O&R	Disagree	Need improved clarity in the definition. Use examples of the common systems and show how they would be categorized. There is too much engineering analysis required to determine if a system belongs in the high or medium category. NERC should consider that certain entities may have facilities that fall under the BES definition for a given region, but because of their own system's characteristics, do not have an impact on the Interconnected BES. There should be an additional category of NA, as with other NERC Reliability Standards. Since the NERC standards apply as per the entity's registration, the entity would then need to provide evidence as to how they categorized the BES subsystems. If all/any BES subsystem elements that are not High or Medium are simply categorized as low, depending on what requirements CIP-003 - 009 bring forward, there could be undue and unjustified entity/consumer costs associated with implementation on BES elements that really do not require such.
Alliant	Agree	
Ameren	Disagree	Not all BES Cyber Systems for a High Impact BES Subsystems that perform functions for the BES should be considered critical. The cyber systems themselves should be evaluated for impact, see our comments on question 6. Yet, this draft standard proposes to categorize all these BES Cyber Systems as critical due to the categorization of the BES Subsystem.
Black Hills	Disagree	Until it is understood how CIP-003 through CIP-009 will be scaled for H - M - L criticality compliance, it is not possible to know whether CIP-002-4 will meet the objective. The concept is good, but not yet clear.

Organization	Yes or No	Question 2 Comment (Response page 14)
TNMP	Disagree	CIP-002-4 does not accomplish the objective because of problems with the current definitions used by CIP-002-4. The current draft is a good first attempt at meeting FERC's concerns; however, definition revisions and other clarifications requested by those submitting comments are needed to help paint the "bright lines" the drafting team is setting out accomplish.
NVEnergy	Disagree	Given the comments in the prior section, there is still some enhancement necessary to adequately accomplish the stated objective. We believe that the categorization as proposed in Attachment 1 to the proposed Standard may inappropriately assign High and Medium impact to various assets/subsystems that are not believed to have such a high degree of impact to the reliable operation of the BES. For example, the continued inclusion of blackstart generation systems as High Impact is in our opinion an overstatement of importance (particularly given that to classify it as such, it would demand the highest level of security protection, when in fact the importance of the blackstart systems is inconsequential except for the extremely rare instance that the systems are in use in a restoration event). We do concur that the basis and concept are correct: the application of security controls should be commensurate with the degree of impact that the subsystems have upon the reliable operation of the BES.
MWDSC	Disagree	Uncertain what, if any, security controls will be applied to a Low BES Impact. Without drafts of CIP-003 through CIP-009, how can CIP-002 be assessed for "applying security control commensurate with the potential impact"?
Empire	Disagree	I do not agree that the categories of Hi, Med, and Low, correctly identify BES Cyber Systems that support the functions critical to the reliable operation of the BES. There should also be a "No" impact category on those items that have no impact on the BES.
NCEMCS	Disagree	I have taken some extracts from existing comments and restated them in full support: The sole purpose of CIP-002 is to identify and categorize cyber systems according to their impact on the BES so we can apply appropriate security requirements to them. The listing of the Cyber System should be based on a top down approach rather than a bottom up approach. Only after a BES Subsystem is classified as a High or Medium Impact, should the Cyber System related to it should be classified as High, Medium Impact. Current CIP standards require an indirect assessment; a simple inheritance of impact from the BES Subsystem to its associated cyber systems without regard for the cyber system's actual function. We think this will result in the over-classification of many cyber systems. Having a purely BES Cyber System focused approach creates the issue of creating an inventory of hundreds of thousands of cyber systems and then performing an impact assessment of each one. This is wasteful of resources and will cause a great deal of work on the industry's part in large part focused on the lowest impact systems. All low impact BES assets have all associated cyber systems classified as low impact. This removes vast amounts of classification work. Since low impact is defined as having NO ability to directly impact the BES in any way, we would propose there be no requirements on this category. There is a danger of unintended consequences where the focus could shift from securing the high and medium impact systems to managing compliance on the several orders of magnitude more numerous 'no impact' systems. In the earlier versions it was a straightforward approach where the Registered Entity identified its Critical Assets (i.e., those assets that could affect the BES) and then you identified the supporting Cyber Assets and then the Critical Cyber Assets. My concern is for example: currently, if an entity determined through their RBAM that they have "no critical

Organization	Yes or No	Question 2 Comment (Response page 14)
		assets", then none of the controls and requirements of CIP-003 through -009 apply. Under this new proposal, let's assume the same entity would declare all assets to be "low impact". What type and level of security controls then apply to these "low" impact assets? None? (As per the old system?) Without information on the level of controls associated with this categorizing scheme, it is difficult to fully evaluate this concept. The V4 standard currently has criteria for High and Medium impacts and lumps all other BES Subsystems into Low, therefore no BES Subsystem nor cyber system is excluded no matter how minuscule its potential impact. If there is even one requirement in the low impact category and that category is auditable and enforceable, the compliance evidence burden placed on entities will be onerous. Since there is no bottom to this standard and low is the 'everything else' category, every cyber system in the BES of North America will be on the list and in scope. There may be tens of thousands of systems per entity (would not each relay be a 'cyber system'?). The majority of your compliance tracking and evidence gathering will be on the lowest impact, but orders of magnitude more numerous cyber systems. If the TFE process also applies to these millions of systems continent-wide we are creating an unmanageable bureaucracy. The standard needs minimum criteria. This has been stated many times I just want to re-enforce it "Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009, or a category for minimal-risk or no-risk subsystems must be created!" Since the Low impact category is simply a catchall, we propose there be no requirements for low.
SWTC	Disagree	Until the BES Definition is resolved, how can an entity identify and categorize BES Cyber Systems.
SCEG	Agree	
Exelon	Agree	
BPA Trans	Disagree	No, we do not agree that CIP-002-4 accomplishes the objective stated in the Purpose statement. The identification and categorization of BES Cyber Systems "commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES" is not achieved. R3.2 requires the Responsible Entity to "assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem." In most cases, this is appropriate as the most important consideration is the reliability of the BES. However, this may lead the over categorization of a BES Cyber System as it is "assigned" the same BES impact, rather than considering whether the effect of the BES Cyber System is significant or not. For example, a BES Cyber System might have Medium or Low BES Impact even though it is associated with a High Impact BES Subsystem.
HQT	Agree	
Allegheny Energy	Disagree	The approach utilized makes an effort to categorize BES assets but does not allow an opportunity to separately categorize BES Cyber Assets. The BES Cyber Asset inherits the impact categorization of the BES asset and creates a one-size fits all solution that may not be commensurate with their potential impact on the BES.
KCPL	Disagree	The goal is a lofty and extremely difficult one to hit. This effort, although noble, does not reflect the level of thoughtfulness required to establish the facility criteria necessary to draw a practical line in the sand to determine reliability impact at a

Organization	Yes or No	Question 2 Comment (Response page 14)
		High, medium or low level. In addition, there needs to be a “No Impact” level. It is not reality to assume that every element or combination of elements has a significant reliability impact.
Connectiv Energy	Agree	The Standard will allow the categorization of BES Cyber Systems, however this alone provides no guidance for what appropriate security controls are. Assuming that CIP-003 through CIP-009 are revised to recognize the categorization then the set will accomplish the larger purpose.
MidAmerican	Disagree	MidAmerican recognizes and understands the intentional shift in purpose from identifying Critical Cyber Asset Identification in CIP-002-2 to BES Cyber System Categorization in CIP-002-4. However, differentiating between high, medium and low may have little value or credibility for many security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the “iron” (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset’s impact (if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. Further, security controls must be applied to distinct, discreet, individual Cyber Assets, not generically defined “systems.” MidAmerican submits there is value in retaining the original purpose from CIP-002-2. MidAmerican’s four proposed changes to CIP-002-2 are presented in question 13.
CPG	Disagree	This proposal does not take into account the criticality of a cyber system to the BES element, nor does it properly take into account the criticality of the BES element to the BES. What is lost in the proposal is that some cyber systems may not be critical to the operation or protection of the BES element, and would therefore not be critical to the BES. To have entities list every cyber system does not have an impact on the safety and reliability of the BES. The generator nameplate criteria, as well as control center MW criteria listed in Attachment 1 seem arbitrary. A discussion as to how those values were developed would be appreciated.
Santee Cooper	Agree	Once the impact levels are fixed, SC does believe it accomplishes the overall goal of protective requirements relative to their impact on the BES.
OGE	Disagree	• The intent is clearly there, however it is difficult to know how to assess the impact the BES due to the terminology. It is too subjective. • This revision, while a reasonable start at carrying out FERC’s direction, does not provide enough meaningful detail so as to make the revised standard something the industry can confidently implement. For example, who decides whether or not something has “directly affected” the BES? What change in voltage for what length of time constitutes an “affect”? What is the difference between “directly affect” and indirectly affect? More definition needs to be provided on these kinds of terms.
Oncor	Disagree	It would appear to provide some additional flexibility, although the specific security controls are not yet defined.

Organization	Yes or No	Question 2 Comment (Response page 14)
PPL Supply	Disagree	Generally agree with EEI Comments. Devices which use a routable protocol that is remotely accessible pose a higher risk than those using a non-routable protocol or are on an isolated routable protocol network.
St. George	Agree	
NGRID	Agree	
MGE	Disagree	Do not agree with the Purpose statement since it does not give the applicable entities the clear and concise requirement(s) in order to fulfill the purpose statement. Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. The loss of a communication link to a BES Cyber System will not automatically cause the inability of equipment and/or electric system's thermo, voltage and stability limits that will cause instability, uncontrolled separation, or cascading failures. Recommend the purpose to read: To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) which could cause instability, separation or cascading to the Bulk Electric System (BES) as a basis for applying security controls.
FE	Agree	Per our prior comments, FE believes the purpose of this standard should be restated as "To identify cyber vulnerabilities that when breached could lead to BES instability, BES separation and/or a cascading sequence of failures." If the team retains its current path, the team should keep in mind that Low BES Impact as defined by this standard indicates a number of things that would NOT occur. The purpose statement is appropriately focused on functions "critical" to the reliable operation of the BES. Therefore, Low BES Impact Subsystems should require minimal or no security controls.
TECO	Disagree	We agree that the draft standard itself would accomplish this if the definitions were clarified, or removed in place of the attachment categorization. The phrase "BES as a whole" should replace BES at the end of the purpose. We also have great concern that the automatic inheritance of impact level of the cyber systems from Attachment 2 to the BES subsystems from Attachment 1 is problematic. This introduces many new cyber systems that do not have direct impact to the reliable operation of the BES subsystems, and is a significant departure from the approach that had previously been communicated by the drafting team. We believe that many cyber systems that currently reside on corporate networks will be pulled into scope. These include systems that do not directly impact BES reliability, that entities may have removed from their control system networks to achieve compliance with the existing set of standards. We foresee the need to create additional electronic security perimeters within corporate networks to accommodate the standards. The goal of these standards should be to protect those cyber systems that are critical to the reliable operation of the BES, not every cyber system associated with the BES.
CECD	Disagree	The purpose should include reference to the effort to categorize BES Subsystems as this is a significant task in this standard.

Organization	Yes or No	Question 2 Comment (Response page 14)
MRO	Agree	N/A
GTC	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Xcel	Agree	
BGE	Disagree	We do not agree. It is too broad and has the potential to capture and bring in to scope items that are not critical to the reliable operation of the BES. The standard is diluted by not focusing on items that are that truly important to the security and reliable operation of the BES. We think that BES Cyber Systems without external computer and communications connections should be excluded. Next day planning systems should not be in scope. We believe that the proposed standard could result in secure BES Cyber Systems, without equivalent physical security protection. For example, it's possible to spend tremendous resources to secure BES Cyber Systems, and leave physical security gaps that would compromise the system.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Although the drafting team has put in a lot of hard work and has tried to help identify and categorize those cyber systems, there's still some ambiguity. As mentioned in the subparts of question 1, we would like further clarification.
TAPS	Disagree	Because the proposed "low impact" category, as currently defined, would sweep in cyber systems that have no potential impact on the reliability of the BES, the standard would, as written, impose significant costs on responsible entities and Regional Entities with no commensurate benefit to reliability. See TAPS response to Question 1.i.
Allegheny power	Disagree	AP believes that it is important and appropriate to apply "security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same

Organization	Yes or No	Question 2 Comment (Response page 14)
		impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations.
FMPA	Disagree	It does come close to doing so, FMPA has some comments on the details of how it is done, including the criteria of Attachment 1. The addition of new terms of "subsystem" and "functions" add complexity and ambiguity. How are these new functions related to the Functional Model, for instance? The real focus ought to be on the worst case contingencies / scenarios that can be caused by malicious manipulation of a cyber system. Such a focus bypasses the need to create new terms such as subsystems and functions. As such, the purpose ought to eliminate reference to the word “functions” and state: “To identify and categorize the BES Cyber Systems that support the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES.”
Duke	Disagree	We believe that the proposed CIP-002-4 is too prescriptive, and that a better approach would be to use the “Cyber First” approach. See all of our other comments on CIP-002-4 for explanation and suggestions for improvement.
NBSO	Agree	
AESI	Disagree	Although the standard defines how to identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the BES, because of the simplistic assignment of impact to the BES Cyber Systems based on the impact of the BES Subsystem with which they are associated, with no other considerations regarding the level of vulnerability posed by a given BES Cyber System, nor the level of impact a given BES Cyber System might have on its parent BES Subsystem, we feel that the standard does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the objective in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with a BES Cyber System. For example, a device without remote access poses a different type and degree of risk than something directly accessible via the Internet. Finally, we believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
IESO	Disagree	Distinguishing between High and Medium is unnecessary and arbitrary. Suggest two levels of cyber security are required : what we’ve got now for the current critical assets (High) and some other less stringent requirements for the rest (the Lows): b. A medium impact includes inability to effectively monitor and control the BES. This can directly cause or create an unacceptable risk of instability, separation, and cascading outages, which is a High impact. c. Medium impact categorization is based on arbitrary generator nameplate rating of 1000 MVA , or voltage level of 200 kV and number of lines with no regard to actual impact. Same for SPS. Thresholds should be determined

Organization	Yes or No	Question 2 Comment (Response page 14)
		according to studies or other criteria determined by the RC. d. The 3 impact levels (H, M, L) create additional layers of complexity for security solutions and monitoring compliance.
Manitoba 2	Disagree	The current wording of the purpose and direction of the standard to include all BES Cyber Systems in the categorization will mean that security controls will be specified for BES Cyber Systems with a categorization of low. Any such identified security controls will then also be auditable. All BES Cyber Systems are not critical to support a BES Subsystem, and as such should not require auditable security controls. Guidance provided to industry on security controls for low impact BES Cyber Systems would be sufficient for the necessary strategic direction and would not require external audit of these low impact security controls. Inclusion of low impact BES Cyber Subsystem as auditable assets in the standard will significantly increase the implementation timeframe, increase the cost and will divert resources required to implement the controls associated higher impact levels. Auditable security controls in CIP-003 through CIP-009 should only be applied to high impact and medium impact BES Cyber Systems.
OMPA	Disagree	The draft standard assumes all cyber systems associated with BES assets have a definite impact on the reliability of the BES. We argue that treating every cyber system associated with a BES asset as a potential impact to the reliable operation of the BES could require extensive controls implementation that would have no net improvement on the reliability of the BES. OMPA urges the drafting team to consider a “no impact” option. OMPA also urges the drafting team to provide drafts of CIP-003-4 through CIP-009-4 for a better understanding of required controls prior to finalizing CIP-002-4.
ATC	Disagree	Suggestion: “To identify and categorize BES Cyber Systems that support functions (Control Center, Transmission Subsystem or Generation Subsystem) that affect the reliable operation of the Bulk Electric System.” Our proposed suggestion is attempting to clarify that the purpose of this standard is to only categorize BES Facilities.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 2 Comment (Response page 14)</th></tr>
<tr><td></td><td></td><td>appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>PSE agrees that the drafting team is headed in the right direction and fully supports their efforts. PSE also feels that not all the BES Cyber Systems have same reliability impact on BES systems. It would be helpful if the drafting team could bring some clarity in this standard to accomplish this objective with no room for interpretation. A BES Cyber System can have no impact for which CIP-002-4 does not seem to allow for especially if there is no remote access to it.</td></tr>
<tr><td>IMPA</td><td></td><td>IMPA has no comments</td></tr>
</table>

Organization	Yes or No	Question 2 Comment (Response page 14)
ERCOT	Disagree	ERCOT ISO recommends that the purpose be revised to address the identification and categorization of BES Subsystems as well as the BES Cyber Systems.
PacifiCorp	Disagree	PacifiCorp recognizes and understands the intentional shift in purpose from identifying Critical Cyber Asset Identification in CIP-002-2 to BES Cyber System Categorization in CIP-002-4. However, differentiating between high, medium and low may have little value or credibility for many security controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just BES one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. Further, security controls must be applied to distinct, discreet, individual Cyber Assets, not generically defined "systems." PacifiCorp submits there is value in retaining the original purpose from CIP-002-2. PacifiCorp's four proposed changes to CIP-002.2 are presented in question 13.
IRC	Disagree	We believe the requirements in CIP-002-4 do not conform to the purpose. Specifically, the purpose focuses on "functions critical to the reliable operation of the Bulk Electric System (BES)". Not all BES Cyber Systems and BES Subsystems that perform functions for the BES are critical. Yet, this standard proposes to categorize all of these Systems and Subsystems and to require protection. The drafting team should eliminate the concept of High, Medium and Low impacts and revert back to the Critical Asset approach. Bright lines for criteria could still be established which we believe will satisfy NERC and FERC concerns regarding the amount of equipment that has been identified as Critical Assets.
PEPCO	Disagree	We are very appreciative of the efforts of the SDT. In particular, we believe that it is important and appropriate to apply - security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES. This draft rightly recognizes that different BES facilities have different potential impacts on the BES. We would suggest however, that not all cyber assets that may be associated with a particular BES Cyber System necessarily have the same impact on the reliability of the BES. We note that devices that use a routable protocol to communicate may have a higher impact than those that do not. Devices that exist within an isolated network segment may have a lower impact that those with access to multiple locations. And devices that have no remote access would have no impact on the BES system. With the draft standard, cyber assets inherit the same category as the BES asset, regardless of communications methods to control the CCA. Assigning BES cyber systems the same impact of the BES Subsystems does not seem appropriate. As was previously mentioned, high, medium or low categorization often has more to do with the connectivity of the asset (e.g. TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (e.g. if it fails, is just one BES asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For BES assets with no remote access, these should be classified as No Impact. If a cyber control system first approach is use, we would offer that the high, medium, or low would not be needed. Appropriate security measures/requirements would be based on the operating platform of the in-scope BES cyber control systems, the connectivity of the asset, and/or the span of control of the cyber asset's impact. At the same time, we would

Organization	Yes or No	Question 2 Comment (Response page 14)
		offer that not all cyber systems need to be considered and would be burdensome to do so. The challenge would be to limit the cyber systems to BES control systems and to identify the in-scope systems (e.g. SCADA, DCS, Microprocessor relays).
NEI	Disagree	A) The purpose as stated is flawed in that it does not deal with cyber vulnerability, which is the whole point of CIPs 002 through 009. NEI believes the purpose of this standard should be restated as "To identify cyber vulnerabilities that when exploited could lead to BES instability, BES separation and/or a cascading sequence of failures." B) If the team retains its current path, the team should keep in mind that Low BES Impact as defined by this standard indicates a number of things that would NOT occur. The purpose statement is appropriately focused on functions "critical" to the reliable operation of the BES. Therefore, Low BES Impact Subsystems should require minimal or no security controls. C) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Summary Consideration: Of the 93 responses for this question, 49 preferred the method in the initial posting, 37 preferred the alternative method, and 7 did not have a preference. Many respondents commented that simplified criteria were needed. Some respondents noted that the standard should provide flexibility to use either approach. One entity noted that both alternatives must be executed in a comprehensive approach. Another entity commented on using CIP-002-3 as a base, expanding to all BES assets and applying the list of asset types in R1.2. Eight entities suggested using an approach based mainly on connectivity and secondarily on control centers and others. Some entities noted that a preference cannot be made in the absence of the controls. One entity proposed a hybrid approach, using a BES impact approach to filter out low impact BES Subsystems, then switching to a BES Cyber System based approach and classify based on the span of control of these BES Cyber Systems. Others cited the matrix approach described in the concept paper.

The SDT considered all comments and has made substantial changes to the requirements in CIP-002-4 (now CIP-010-1) to allow an entity to use any approach to reach the goal of the final categorization of BES Cyber Systems. The new requirements are drafted with more focus on the objective and desired outcome, rather than on the methodology or process.

Organization	Yes or No	Question 3 Comment (Response page 15)
Progress Energy	Prefer method proposed in the standard	A proper judgment cannot be made on the proposed methods without knowing the ultimate impact of the other Version 4 CIP-003 through -009 standards. Both methods would ultimately require a full inventory of all BES assets and this process will not improve the overall reliability of the BES. If the proposed changes to the definition of Cyber System are made ("A discrete set of one or more routable or dial-up programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data."), then we are in agreement with the method proposed in the Version 4 standard.
Dynegy	Prefer method proposed in the standard	
GSOC/OPC		We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Hayden	Prefer alternative	A decision tree / flow chart approach would be more effective and probably would provide more consistent results between Registered Entities.

Organization	Yes or No	Question 3 Comment (Response page 15)
	method	
SDGE	Prefer alternative method	
APPA	Prefer alternative method	APPA Task Force Comments: We believe each utility will need to inventory all BES connected Cyber Systems and then determine their level of impact on the BES based on the criteria in Attachment 1. See comments submitted in response to Question #6 below.
Consumers		Although we prefer the method proposed in the standard, substantial changes must be made in the process to gain our full support of the method. The suggested alternative method simply results in far too much analysis and documentation and appears as if it would result in the same list of assets that needs to be protected, yet through a much more onerous path. As noted earlier though, the current proposed method must be changed to allow for the separate (from the subsystem categorizing) secondary categorizing of the cyber assets. Neither method is recommended. The existing CIP-002-3 accomplishes what is needed. Taking a new course will lead to confusion and not result in any improvement in what has been accomplished to-date. If the concern is protecting the reliable operation of the BES, why is it not sufficient to have two categories of assets as in CIP-002 versions 1 through 3? Either something is critical or it's not... No matter how we choose to categorize and wordsmith, at the end of the day the same components will affect the reliable operation of the BES. Changing CIP-002 at this stage of the game is not going to reduce administrative overhead.
NPCC	Prefer method proposed in the standard	
MPPA	Prefer method proposed in the standard	
Central Lincoln	Prefer method proposed in the standard	You must categorize the electrical facilities prior to categorizing the associated cyber equipment.
Dominion	Prefer method proposed in the standard	Dominion recommends that BES assets be evaluated first and then the cyber systems (functions) be evaluated based on the criticality of the associated asset.
Encari	Prefer method proposed in	The proposed method provides for specific scope limitations that are necessary during the discovery process, the alternate method would lead to an unnecessary inventory or nearly unlimited scope during the process. We are

Organization	Yes or No	Question 3 Comment (Response page 15)
	the standard	concerned about the transition process between the current CIP standards and version 4 as the identification of any additional Cyber Assets at this time only allow for one level of criticality whereas the new standard defines 3 levels. If version 4 of CIP-002 is to be adopted without updating the remaining CIP standards simultaneously it will lead to confusion as to which requirements pertain to which Cyber Assets. We recommend developing a mapping of the current mandatory requirements to the 3 categories. The proposed method also is missing specific elements within attachment 2. For instance, we have identified situations where BES Cyber Systems included for reducing emissions may impact a BES Subsystem indirectly. We also recommend further addressing security controls for remote vendor support as it is incredibly important for day to day operations and emergency conditions. Although indirect components can lead down a very difficult path to properly inventory and limit, these cases should be reviewed for inclusion.
US ACE – NW	Prefer method proposed in the standard	
SCE	Prefer alternative method	Since the genesis of the NERC CIP standards was the protection of BES assets by providing security to the cyber assets supporting BES functions, SCE believes that risk analysis should be driven by the function of the respective BES assets. A cyber asset first approach should be used to identify connectivity types and cyber asset functionality based on Attachment 2. The level of security controls can then be determined based on BES criticality as identified in Attachment 1.
USBR	Prefer alternative method	This question is poorly worded in that you cannot disagree with Attachments 1 or 2, which happens to be the case. As indicated in previous answers the alternative method is create a criteria for assessing impacts of elements. This proposed process can easily result in over categorization of elements which will not result in increased reliability. The focus needs to be on those functions which can harm the reliability of the BES (have an impact. This standard touches on some of the issues which need to be addressed in the assessment criteria. It is unrealistic to assess 20 MW units against a 2000 MW requirement. However, the responsible entity (lets say GO) should communicate with its TO, BA or RC, to determine if the TO, BA, or RC relies on the facility for specific reliability functions (AGC or AVC). In some WECC balancing authorities a 200 MW Pump Storage plant may be relied heavily for AGC. On other WECC balancing authorities 200MW is decimal dust.
Dyonyx	Prefer method proposed in the standard	While we prefer the proposed method in the standard, we believe there is some risk that independent “Elements” that are not directly related to a specific BES Cyber System may be missed if a complete inventory is not conducted.
MISO	Prefer method proposed in the standard	
Westar	Prefer method proposed in	

Organization	Yes or No	Question 3 Comment (Response page 15)
	the standard	
Green Country		Neither to do a proper assessment you would have to work it both ways to make sure all were included. Again no "Bright Lines" are drawn. Also to preclude an interpretation. Do you have to only have 1 sub element in for example Dynamic Response to have a Dynamic Response function? i.e. Power system stabilizers and nothing else. OR Must you have all of the sub elements listed for each respective function?
Oregon PUC		No comment
NB Power Gen	Prefer method proposed in the standard	
Manitoba 1	Prefer method proposed in the standard	Need more time to review
Portland GEG	Prefer method proposed in the standard	PGE does not have a preference, however, we are marking that we prefer the method in the standard because it is most similar to current methodology.
PSEG	Prefer method proposed in the standard	Comment #1: After reviewing both approaches, they seem to result in the same list of BES Cyber Systems. Comment #2: The existing CIP-002-3 accomplishes what is needed. Taking a new course will lead to confusion and not result in any improvement in what has been accomplished to-date. Comment #3: 1. Criterion 1.3. would assign a “High BES Impact” to generators that have been “pre-designated” as Reliability Must Run units. Whether a generator is High Impact, Medium Impact, Low Impact or No Impact has nothing to do with the label an RTO/ISO slapped on it to keep it from being retired. The assignment of “High BES Impact” should be based on a sound engineering evaluation, not on a label. 2. Criterion 1.11. refers to “frequency related instability.” There is no such thing as “frequency related instability” for transmission. The accepted categories of transmission stability are as follows: (1) steady-state stability; (2) transient stability; (3) small signal stability; (4) voltage stability. This error can be fixed by simply deleting the words “due to frequency related instability.” 3. With the recommended fix to Criterion 1.11. (see (3) above) Criterion 1.10. can be deleted. 4. Attachment 1 uses a number of euphemisms to refer to undesirable outcomes, e.g. “electric system collapse,” “complete operational failure of the transmission system” and “separation.” The authors of Attachment 1 need to stick to terminology found in the lexicon of power system engineers and clearly communicate just what the standard is.

Organization	Yes or No	Question 3 Comment (Response page 15)
		The indiscriminate use of vague terminology in standards will lard up the cost structure of competitive generators with no possibility of recovery. 5. Criterion 1.7. is way off the mark. The fact that a contingency requires implementation of a TLR says nothing about whether the facility is High Impact, Medium Impact, Low Impact or No Impact. TLRs are routinely implemented in operational circumstances that have no impact at all. This Criterion needs a lot of work; as written it arbitrarily assigns "High Impact" status to events that are routinely encountered in the day-to-day operations. Overall, Attachment 1 needs addition rework. Generators must be sensitive to the needs of the competitive business they are in and not be subjected to cost increases that add little enhancement to overall reliability. Vagueness and ambiguity will undermine the competitive business generators are in. With proper attention to precise engineering terminology and performance instead of generalities, the number of criteria in Attachment 1 can be greatly reduced.
WE-Energies	Prefer alternative method	Wisconsin Electric Power Company supports EEI's comments regarding this question. In addition, we support an alternative approach as put forth by several entities. This includes the use of a "cyber first" approach to asset classification and impact to the BES. This would include: • Identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment 2. • Identification of control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate as "high impact" cyber assets to the BES • "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use would be classified as "medium impact" cyber assets.
Idaho Power	Prefer alternative method	The criteria in Attachment 1 is more applicable to categorization of BES subsystems than BES Cyber systems. Another alternative would be to inventory BES cyber systems and categorize by their impact on the critical functions.
SOCO	Prefer alternative method	In the matter between the BES Subsystem focus vs. the BES Cyber System focus, Southern Company supports a hybrid approach. The sole purpose of CIP-002 is to identify and categorize cyber systems according to their impact on the BES so we can apply appropriate security requirements to them. In order to accomplish this, we need to know the impact of the cyber system, not solely the impact of BES Subsystems. Current CIP standards require an indirect assessment; a simple inheritance of impact from the BES Subsystem to its associated cyber systems without regard for the cyber system's actual function. We think this will result in the over-classification of many cyber systems. For example, a high impact substation may contain a fault recorder whose function is to collect data for future analysis and a relay on a 500kV line to a peer utility. The impact to the BES of those two cyber systems are vastly different and both do not need to be declared high impact and meet all the same requirements due solely to the substation's impact level.

Organization	Yes or No	Question 3 Comment (Response page 15)
		However, having a purely BES Cyber System focused approach creates the issue of creating an inventory of hundreds of thousands of cyber systems and then performing an impact assessment of each one. This is wasteful of resources and will cause a great deal of work on the industry's part in large part focused on the lowest impact systems. We propose a hybrid approach: 1. The Planning Authority performs an engineering analysis utilizing 'bright line', well-defined parameters that are consistent across the interconnection. The result of the engineering analysis is a list of BES assets classified according to impact. Bright line parameters would also have to be determined for control centers based on the aggregate of controlled assets. 2. All low impact BES assets have all associated cyber systems classified as low impact. This removes vast amounts of classification work. Since low impact is defined as having NO ability to directly impact the BES in any way, we would propose there be no requirements on this category. There is a danger of unintended consequences where the focus could shift from securing the high and medium impact systems to managing compliance on the several orders of magnitude more numerous 'no impact' systems. 3. For the medium and high impact BES assets, we switch to the cyber system focused approach. The associated cyber systems are inventoried and each is classified as to its direct impact based on their "span of control"; how many MW's of load or generation are at risk from this cyber system should it be compromised, misused, or degraded. In conclusion, we use the BES Subsystem/Engineering Analysis approach as a first filter to quickly handle the quantities of low impact cyber systems, then we switch to the BES Cyber System focus to get a truer impact determination for the medium and high impact cyber systems. The control system for a Generation Unit may be classified as a High Impact, but classification of a condenser air in-leakage monitor, which is neither remotely accessible nor essential for generation should not required to be classification at the component level.
DTE	Prefer method proposed in the standard	Either method should produce the same list.
AEP	Prefer alternative method	Refer to question #2 above.
Edison Mission	Prefer method proposed in the standard	While we prefer the proposed method in the standard, we believe there is some risk that independent "Elements" that are not directly related to a specific BES Cyber System may be missed if a complete inventory is not conducted.
Calpine	Prefer method proposed in	

Organization	Yes or No	Question 3 Comment (Response page 15)
	the standard	
NS&T	Prefer alternative method	We believe it is appropriate to consider impact(s) on BES, but we believe impact criteria should be simplified.
E ON	Prefer alternative method	Attachment 1 provides a list of facilities to be classified as High and Medium impact BES Subsystems. That is all that should be needed. Attachment 2 includes functions, such as providing reserves and facilities used in shedding load that would render nearly every generating unit or distribution feeder critical to BES reliability. That is not the case and the costs of proceeding in this manner promise to far outweigh the incremental enhancement to BES reliability, if any. E ON U.S. notes that CIP-002 Attachment 1 section 1.2 is unclear as to whether the reserve obligation is that of the reserve sharing group or the participating member. It should be of the group as a whole otherwise the economic and operational benefits of reserve sharing could evaporate. This would of course depend on the requirements of the as yet unseen CIP-003-009 V4 standards. Section 1.7, 1.8, 1.10, 1.11, 1.12 should be limited to an appropriate planning scenario. There is no end to the operating scenarios one might conceive that would result in the sorts of adverse reliability outcomes these sections each describe. At some point risk has to be defined in a rational and objectively measurable manner. Section 1.6 should be limited to an identified primary Cranking Path as opposed to all conceivable Cranking Paths.
Carthage	Prefer method proposed in the standard	CWEP feels that Attachment 2 should be eliminated because it causes confusion. CWEP feels that the functions listed in Attachment 2 should be specifically covered in Attachment 1 under the impact categories they fit. The way the attachments are designed leaves too much room for interpretation. CWEP is okay with the format of the standard but would like for the criteria to be more specific.
WECC	Prefer alternative method	The First method provides a simpler method of generating a list, and would be easier to audit to the standard. The alternative method provides for a more comprehensive evaluation and could potentially find assets that are critical to the BES that are not specifically classified in Attachment 1 or that are identified at a later time without needing to update the standard. If the alternative method were used, Requirement 3 would need to be updated to match.
Entergy	Prefer alternative method	The purpose of CIP-002-4 is to define the process Responsible Entities must use for identifying in specific terms the 'scope of applicability' of the rest of the CIP Standards for the grid infrastructure owned/operated by each Entity respectively. This process should approach the matter using a logical top-down methodology, beginning with identification of "Functions Essential to Reliability of the BES" as identified in Attachment II to the CIP-002-4 draft standard. From there, the method should proceed with identification of cyber assets used to implement said "Functions," followed by categorization of those cyber assets based upon potential adverse impact on reliable operation of the BES (as a functioning 'system') posed by the different types of cyber assets themselves. It's the potential impact of various cyber exploits or compromises presented by different types of cyber assets that dictate the need for a hierarchy of security controls and countermeasures, not categorization of BES equipment, sites, etc. based on type, size, facility rating, etc.

Organization	Yes or No	Question 3 Comment (Response page 15)
CenterPoint	Prefer method proposed in the standard	Although CenterPoint Energy believes the asset-based methodology in the existing version of CIP-002 is preferable to the subsystem-based methodology proposed in version 4, CenterPoint Energy believes the method proposed in version 4 is preferable to the alternative approach presented in this question.
LCRA	Prefer method proposed in the standard	
FRCC		As noted in a previous comment, I am not sure why you need the definitions of subsystems etc since you have specific criteria identified in both Attachments.
NIPSCO	Prefer method proposed in the standard	After reviewing both approaches, they seem to result in the same list of BES Cyber Systems. Suggestion: Clarify what the SDT views would be the impact of reversing the approach.
ConEd	Prefer method proposed in the standard	
EEI		EEI believes that while there may be some value in identifying and characterizing significant facilities such as large generating facilities, large transmission substations, or control centers, the real opportunity is to identify and characterize the cyber systems that are required to keep these facilities and functions operational.
O&R	Prefer method proposed in the standard	With consideration of comments in question 2.
Alliant	Prefer method proposed in the standard	We agree with the method in principle, however, see answers to questions 8 and 12 for specific comments on Attachment 1 and 2 criteria.
Ameren	Prefer method proposed in the standard	Responsible Entities should be allowed the choice of either method. Until a thorough analysis is performed by each entity, they should be allowed the option to define their methodology either way. If we had to choose today without time to evaluate each option we would select the proposed method. In either case Attachment 1 and Attachment 2 need to be modified as suggested in our comments in questions 8 and 13.
Black Hills	Prefer method proposed in the standard	Regardless of the order processed, both categorizations must be completed. The process will likely be iterative, so the order doesn't matter. The approach described in CIP-002-4 most closely matches the work done by entities already, which is the basis for BHC's preference.
TNMP	Prefer method	TNMP finds the proposed standard method more manageable than the alternative of inventorying all BES Cyber

Organization	Yes or No	Question 3 Comment (Response page 15)
	proposed in the standard	Systems. Keeping track of BES Cyber Systems for BES Subsystems that are of Low BES Impact would take away the limited manpower to focus on maintaining massive documentation for an audit and exposes Entities to findings that are not significantly relevant to the security of the BES. If a Responsible Entity had far more Low than High or Med BES Impact Subsystem then much time would be spent maintaining documentation for an audit. Why spend the time for a system that is recognized as having Low BES Impact and thus probably would not be subject to future CIP-003 through CIP-009 revisions? Let the Responsible Entity use its resources to focus on the BES Cyber System that are more likely to have a High/Med BES Impact.
NVEnergy	Prefer alternative method	The security controls prescribed by the subsequent CIP Standards must be targeted toward those cyber systems that are essential to the reliability of the BES and are associated with a function of the BES subsystem that has significant impact on the BES. Given that the engineering and planning of the BES is such that single contingency failures can be accommodated under the most extreme circumstances, categorization strategies for the CIP purposes that begin with the classification of the BES facilities is inappropriate. The revised CIP standards should focus first upon the cyber devices that can be compromised; then proceed to a determination of what degree of impact that compromise might have upon the BES.
MWDSC		Prefer none of the above. Recommend separating the transmission from generation criteria in the attachments and including more specific technical criteria such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Prefer alternative method	A preferred method would be: Step 1-Inventory all BES Cyber Systems Step 2 Identify all related BES Subsystems Step 3-Categorize based on Attachment 1 Step 4-Notify neighboring TO Step 5- Review and update lists
SWTC	Prefer alternative method	
SCEG	Prefer method proposed in the standard	
Exelon	Prefer alternative method	Exelon believes that the standard should first consider the cyber system vulnerabilities and then determine the potential impact to the reliability of the BES.

Organization	Yes or No	Question 3 Comment (Response page 15)
BPA Trans	Prefer method proposed in the standard	We marked "Prefer method proposed in the standard" as it most closely matches the current Critical Asset and Critical Cyber Asset methodology. It appears that definitions described in the rest of the document allows BES Cyber Systems to be classified as BES Subsystems. We do not believe that this is correct. Cyber Systems support the reliability functions of the BES Subsystems, not the other way around.
HQT	Prefer method proposed in the standard	
CCG	Prefer alternative method	Concerns remain about whether this approach effectively addresses reliability vulnerabilities without unnecessarily requiring controls on assets that do not impact reliability. We support further development and consideration of an approach that starts with an analysis of cyber assets.
Allegheny Energy	Prefer method proposed in the standard	
KCPL	Prefer alternative method	Attachments 1 and 2 are good lists of all the reasons to determine and provide protections for the cyber infrastructure underlying the monitoring and control of the BES. However, neither of these attachments in any combination are sufficient to provide the level of guidance necessary to draw appropriate conclusions. The way this is proposed could involve every generator, transmission line, bus, breaker and transformer. Apparently, it is not sufficient for Registered Entities to develop a process for the determination of reliability impact of their facilities and this proposal does not sufficiently establish the criteria to make that same determination. Although I do not disagree with the concepts being promoted here, namely a process to classify facilities and equipment such as HIGH, MEDIUM, and LOW, the criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to "plug into" this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
Connectiv Energy	Prefer method proposed in the standard	
MidAmerican	Prefer alternative method	1. Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. 2. Change CIP-002-2 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in

Organization	Yes or No	Question 3 Comment (Response page 15)
		CIP-002-2. 3. Change CIP-002-2 R3 to use “the list of BES assets” instead of “the list of Critical Assets.” Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility. 4. CIP-002-4 must be implemented on the same schedule as revised security controls. 5. Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunities to move forward with CIP-002 and to prove what categorizations will be meaningful. The existing work from the proposed approach would then be validated or revised based on its applicability to the security controls.
CPG	Prefer alternative method	The prior version of CIP-002 considered two dimensions of risk. The first dimension of risk considered was impact, which was whether or not a cyber asset was associated with a critical asset. Secondly, it considered vulnerability by determining whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal, the SDT has eliminated any consideration of the risk due to vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest categories of varying degrees of vulnerability (high and low) be added to the criteria in Attachment 2. Furthermore, understanding the design basis threat against which mitigation measures may be built is fundamental in creating an effective set of control measures. The threat potential basis should be clearly established. In addition, time and effort should be given to development and consideration of a “cyber first” approach. We appreciate that the proposed version seeks to protect the assets most critical to the bulk electric systems. However, the direction of this proposal may be missing some vulnerabilities and drawing some assets into scope that have little if any impact on reliability. For any approach taken, it is important to remain focused on reliability.
Santee Cooper	Prefer alternative method	Also noting that both Attachments need re-work.
OGE	Prefer alternative method	I would prefer a hybrid where you categorize the BES Subsystems and then assess the risk of the cyber assets and the potential impact on the BES Subsystem.
Oncor	Prefer alternative method	More intuitive approach.
PPL Supply	Prefer	Agree with EEI comment.

Organization	Yes or No	Question 3 Comment (Response page 15)
	alternative method	
St. George	Prefer alternative method	We are also very concerned about the timetable of CIP-002-4 in relation to the accompanying standards CIP-003 through CIP-009. Entities should be able to know the requirements imposed on certain classifications before commenting on criteria that place entities in said classifications. CIP-002-4 comments should be open during the same period as CIP-003-4 through CIP-009-4.
NGRID	Prefer alternative method	The reference framework of electric grid engineering, facilities ratings, etc listed in Attachment 1 is not required and the alternative method sans the Attachment 1 criteria will be a better approach since the issues at hand needs to be approached from a networked-computing systems security engineering perspective.
MGE	Prefer alternative method	A NERC Standard only needs to state “what” has to be accomplished not “how” the entity shall meet the requirements. This question is not in line with the actual requirements of 1 and 3. Both R1 and R3 start with “As a step in…”. Neither requirement states that R1 or R3 have to follow any order, the requirements do state that R1 and R3 are steps (processes) used to identify categorize an entity’s BES Cyber Systems. Please clarify this question.
FE		We do not prefer either alternative as indicated above. The use of the term "Subsystem" in Attachment 1 and the various Subsystem definitions that include direct linkage to a Cyber System ensures that Attachment 1 is not merely a "Big Iron" approach of categorizing electric grid assets ignoring Cyber Systems. Therefore, the existence of a Cyber System is a prerequisite to its Subsystem components that are being considered. In other words, a cyber review is not something that would occur subsequently. Rather than having Attachment 1 drive a High/Medium/Low categorization FE proposes that Attachment 1 appropriately provide the Subsystems that if compromised could lead to a High BES Impact (cascade, instability, etc.). Accordingly we propose a re-work of Attachment 2 such that it would direct appropriate High/Medium/Low categorization for controls and countermeasure requirements in CIP-003 through CIP-009 that reflect the differences in the Cyber System classification. In layman terms, routable technologies would be High, dial-up Medium and legacy serial communications would be Low. FE believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
TECO	Prefer alternative method	We support the “Cyber First” methodology as described in Entergy’s Comments. We believe that this will drive a matrix approach to include both the impact and risk of probability of exploitation associated with the cyber system. We believe that the impact level of the cyber system should be directly tied to the load controlled by that cyber system. We believe that routable protocols that could be used in sophisticated or coordinated attacks against a large portion of the grid should be considered higher risk of exploitation and serial or non-routable protocols that would be limited to targeted attacks on specific equipment should be afforded a lower risk. Entergy’s comments further explain this approach. If this methodology is adopted, we believe that much of the concern about specific Critical Assets related to generation

Organization	Yes or No	Question 3 Comment (Response page 15)
		would be resolved. We also believe that much of the current CIP002 V4 draft would change, which in turn would change our consideration of the other questions on this comment form.
CECD	Prefer method proposed in the standard	Subject to modifications as described, including the ability to identify assets that have no BES impact, CECD supports a process for evaluation of the BES assets impact on the system prior to engaging in listing BES Cyber Systems. CECD does not encourage a cyber first approach to the extent such an approach jeopardizes the BES threshold which is very important to prevent an overly broad application of these requirements, including impact to demand response programs at the consumer level.
MRO	Prefer method proposed in the standard	We agree with the method in principle, however, see answers to questions 8 and 12 for specific comments on Attachment 1 and 2 criteria.
GTC		We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
Xcel	Prefer method proposed in the standard	
BGE	Prefer alternative method	We feel that a better sequence for identifying high impact BES subsystems would be to start with an analysis of cyber assets to first evaluate those systems that control or impact operations of the BES, rather than starting with generation or transmission assets, and determining which of those are high impact. To the extent that Attachment 1 remains a part of the standard, we offer the following revisions: (High Impact BES Subsystems): 1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or Low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability “must run” units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan. Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each

Organization	Yes or No	Question 3 Comment (Response page 15)
		Generation Subsystem. 1.5. Each Transmission Subsystem that contains switching stations substations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines leaving the station. 1.6. Each Transmission Subsystem comprising the Cranking Paths. 1.7. Each Transmission Subsystem that, if lost, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method consistent with FAC-10. 1.8. Each Transmission Subsystem that, if lost, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We feel that 1.9 was duplicative with the presence of 1.1-1.4 and 1.8 1.9. Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above. The group felt that 1.10-1.12 were duplicative with the presence of 1.7 1.10. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse as determined through an engineering evaluation or other assessment method. 1.11. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. 1.12. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages. 1.13. Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions

Organization	Yes or No	Question 3 Comment (Response page 15)
		for transmission assets or generation assets of 2,000 MW or more New proposed element: 1.17. Each BES Subsystem whose loss qualifies as a category C or D event according to TPL-001-1. * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and that functional entity submits a written request for the information. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments.
Springfield, MO	Prefer alternative method	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Prefer method proposed in the standard	
TAPS		See TAPS response to Question 1.a.
Allegheny Power	Prefer method proposed in the standard	
FMPA		Neither. Both the concepts of Subsystems and functions are unnecessary and add confusion and complexity to the standard. The focus of the standard ought to be on the Cyber Systems themselves, and the criteria for which we define High, Medium and Low BES impacts to those Cyber Systems. Instead, we recommend identifying the worst case contingencies / scenarios that can be caused as a result of a Cyber System rendered unavailable, degraded or compromised, and compare the contingencies / scenarios with the criteria of Attachment 1. In this way, we assign High, Medium and Low impact directly to Cyber Systems without unnecessary middle steps of defining Subsystems and functions. This, of course, would require an inventory of Cyber Systems, but, such an inventory would already be necessary to enable the definition of Subsystems anyway, so, defining Subsystems is an unneeded step in the process.
Duke	Prefer alternative method	We believe that an alternative method is preferable. The first step should be to identify the BES Cyber Systems that can impact functions which are essential to BES reliability. By beginning with an examination of what the various interconnected Cyber Systems can affect, and then ranking them based upon their potential impacts, an entity can better determine the direct impacts, aggregated impacts due to interconnection, as well as common mode vulnerabilities.

Organization	Yes or No	Question 3 Comment (Response page 15)
NBSO	Prefer method proposed in the standard	
AESI	Prefer alternative method	We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits.
IESO	Prefer method proposed in the standard	
Manitoba 2	Prefer method proposed in the standard	The cyber-up approach creates a list of a large number of assets which would need to be auditable and managed for any changes.
OMPA	Prefer alternative method	For Requirement 1, OMPA suggests "…each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria …". Many entities are owners that do not operate the BES subsystems. Security controls should be based on operation, not ownership.
ATC	Prefer method proposed in the standard	
LES	Prefer method proposed in the standard	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 3 Comment (Response page 15)</th></tr>
<tr><td></td><td></td><td>security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Prefer method proposed in the standard</td><td>It is imperative that the standard effectively achieves the proper security controls and ensures reliability without being requiring resources to focus on documenting, evaluating, and categorizing what is not really important. It seems that the proposed method of categorizing high and medium BES Subsystems and then determining BES Cyber Systems based on critical functions identified in Attachment 2 and bounded by points of vulnerability associated with remote access would ensure entities focus on the important things.</td></tr>
<tr><td>IMPA</td><td>Prefer method proposed in the standard</td><td></td></tr>
<tr><td>ERCOT</td><td>Prefer method proposed in the standard</td><td></td></tr>
</table>

Organization	Yes or No	Question 3 Comment (Response page 15)
PacifiCorp	Prefer alternative method	1. Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. 2. Change CIP-002-2 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in CIP-002-2. 3. Change CIP-002-2 R3 to use "the list of BES assets" instead of "the list of Critical Assets." Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility. 4. CIP-002-4 must be implemented on the same schedule as revised security controls. 5. Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunities to move forward with CIP-002 and to prove what categorizations will be meaningful. The existing work from the proposed approach would then be validated or revised based on its applicability to the security controls.
PEPCO	Prefer alternative method	Modified cyber approach: If a cyber control system first approach is use, we would offer that the high, medium, or low would not be needed. Appropriate security measures/requirements would be based on the operating platform of the in-scope BES cyber control systems, the connectivity of the asset, and/or the span of control of the cyber asset's impact. At the same time, we would offer that not all cyber systems need to be considered and would be burdensome to do so. Please reference discussion of Cyber System. We would propose a method that would identify the BES Cyber Control systems. These should be limited and the in-scope systems (e.g. SCADA, DCS, Microprocessor relays) should be identified. With the standards identifying appropriate security measures/requirements based on specific criteria (e.g. operating platform, connectivity of the asset, span of control of the cyber asset's impact) there would be no need to review the big iron other than for the span of control. We believe that this modified cyber first approach would mitigate the administrative burden of the existing cyber security standards and the proposed methods and get closer to the goal, the purpose of the standards, and moves us toward performance based requirements.
NEI	Prefer alternative method	A) This process should approach the matter using a logical top-down methodology, beginning with identification of "Functions Essential to Reliability of the BES" as identified in Attachment II to the CIP-002-4 draft standard. From there, the method should proceed with identification of cyber assets used to implement said "Functions," followed by categorization of those cyber assets based upon potential adverse impact on reliable operation of the BES (as a functioning 'system') posed by the different types of cyber assets themselves. It is the potential impact of various cyber exploits or compromises presented by different types of cyber assets that dictate the need for a hierarchy of security controls and countermeasures, not categorization of BES equipment, sites, etc. based on type, size, facility

Organization	Yes or No	Question 3 Comment (Response page 15)
		rating, etc. B) Alternative Top-down argument for defining the correct CIP Standards' Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue. • N-1 engineering also dictates that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on the perpetrator's ability to *navigate* across and between control system data networks to *access* multiple sites. C) Another Alternative: The existence of a Cyber System is a prerequisite to its Subsystem components that are being considered. In other words, a cyber review is not something that would occur subsequently. NEI proposes a re-work of Attachment 2 such that it would direct appropriate High/Medium/Low categorization for controls and countermeasure requirements in CIP-003 through CIP-009 that reflect the differences in the Cyber System classification. In layman terms, routable technologies would be High, dial-up Medium and legacy serial or other non-routable communications would be Low. NEI believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. D) Need to define screening criteria for when cyber applies. E) Need to clarify "the potential to adversly impact". F) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems.

1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."

Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: Of the total of 93 respondents, many commented again on the need to know the impact of controls. A number of respondents commented on the requirement for the Reliability Coordinator (RC) to approve engineering analyses: these commenters noted that RCs should be removed from these criteria. Some suggested that the Planning Coordinator is better suited for that role. Others commented that criteria for evaluation of engineering analyses were needed and that approved engineering analysis methodologies should be published. Some suggestions were made to specify a blanket option for engineering analyses to all criteria.

There were a number of comments on the requirement for update, many on the amount of time specified before a change in the electric system is reflected. There were comments about the vagueness of the concept of BES Subsystems, and about questions of joint ownership, since the requirements focus on asset ownership. There were also comments on the open ended nature of the word "any" in the requirement.

The SDT considered these comments and has made substantial changes to the requirements. With a direct BES Cyber System to criteria for impact approach, the traditional use of BES impact engineering analyses becomes unnecessary for the evaluation of BES Cyber Systems, nor does any widely used methodology exist for that purpose. The criteria is now be based on bright lines and the impact categorization based on that of the BES Cyber Systems on the functions provided by BES Facilities.

The requirement for reviewing the categorization is now a separate requirement and based on changes in the BES Facilities that the entity owns or operates. The update period has also been extended to 60 days.

Organization	Yes or No	Question 4 Comment (Response page 16)
Progress energy	Disagree	We cannot agree with the categorization without knowing the ultimate impact of the CIP-003 through -009 Version 4 standards.

Organization	Yes or No	Question 4 Comment (Response page 16)
		Change 1.1 from "…within 30 calendar days of the completion of the change" to "…on an annual basis".
Dynegy	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets."
GSOC/OPC	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing "within 30 calendar days of the completion of the change" with "within 30 calendar days of the Responsible Entity becoming aware that the change has occurred". Also, to clarify applicability, we suggest replacing the phrase "that could affect the impact of BES Subsystems" with "that could affect the degree of impact of the Responsible Entity's BES Subsystems." For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
SDGE	Disagree	We are advising that the 30 day timeframe is too short for the work that needs to be completed. The 30 days typically includes the time required to do studies and then get approval from the Reliability Coordinator. We suggest the 30 day timeframe apply to providing the study results to the RC. While commissioning of new BES Subsystems is addressed, the acquisition of existing BES Subsystems is not addressed in R1.
APPA	Disagree	We disagree with the need for BES Subsystem identification as discussed below under Question #6.
Consumers	Disagree	Under the proposed regulation, in order to properly classify a generation subsystem, the generator owner and generator operator need to be provided information from the transmission operator and reliability coordinator. There are no requirements in the proposed standard for the transmission operator or reliability coordinator to provide such information. Without such requirements in the standard, the generator owner and generator operator should not be held liable for non-compliance due to failure of the transmission operator and reliability coordinator to provide the required information. The requirement in R1 should be modified because the goal is not to identify "appropriate security controls for its assets", but rather the same for its critical (high impact, essential, call it whatever) cyber assets or cyber systems. The requirement for producing a list has not yet been introduced within the document. A list is discussed in R3, but that is a list of cyber systems.

Organization	Yes or No	Question 4 Comment (Response page 16)
		On the surface, 30 days seem to be a reasonable time-frame to update the (yet undefined) list. However, we are concerned that some projects to place a subsystem in service (such as a small change or addition to and existing facility) may not give adequate time for all the ensuing requirements that come from CIP-003 >> CIP-009. In addition, there are REs that currently only have Control Centers (and associated Cyber Assets) and a few substations (with NO critical cyber assets) as critical, so these REs have not had to implement CIP-003 >> CIP-009 in a field environment. As one can imagine, doing so if a far greater challenge than the controlled environment of a control center and will be much more difficult. The 30 day period would not be nearly adequate time to implement cyber security controls in this instance. As such, we suggest the requirement be change to at least 60 days. The inclusion of "… or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System" is too vague as a trigger for having to update the list. Specific criteria needs to be introduced instead. We believed the annual review of the critical asset list and critical cyber asset list in the previous versions of the standard was appropriate and such a review should be required here as well.
NPCC	Disagree	RC should be removed from 1.2.
SWPA	Disagree	Updating the categorized list of BES subsystems within 30 calendar days of completion of any change to a BES subsystem is too short a time period for Responsible Entities to assess the impact of the change and update its list. Suggest lengthening the time period from 30 days to 90-120 days.
MPPA	Agree	MPPA concurs with the intent of the requirement, but that R1.2 needs to be clarified. 1) The engineering evaluation or other assessment method needs standardization so it is applied consistently throughout the industry. 2) Does the responsible Entity develop a methodology to be approved by the Reliability Coordinator or Reliability Assurer? Or, does the Reliability Coordinator or Reliability Assurer provide an approved methodology to be used by the Responsible Entity? As written, this requirement does not clarify who provides the assessment method.
Central Lincoln	Disagree	Central Lincoln fails to see why the yearly requirement of the present version presents an unacceptable risk to reliability. This will be a burden on those entities that are actively updating their systems, and will provide a disincentive to do so. This could harm rather than improve reliability. 1.2 is ambiguous. Must the "engineering evaluation" be approved by the Reliability Coordinator or Assurer, or just the "other" method(s)? From the webinar, it seems the SDT intended that both need approval, but this is not clear in the standard as written. There is presently no requirement for RCs or RAs to perform any assessment of an entity's evaluation. CIP-002 or another standard should include a requirement for RCs/RAs to perform these assessments when asked, and within a

Organization	Yes or No	Question 4 Comment (Response page 16)
		reasonable time period of such a request. As written, the standard expects registered entities to produce the approvals of other entities not under their control and under no obligation to help.
NERC	Agree	1. In order to support compliance activities, add the following and update the Measures section appropriately: R1: add text to require signed and dated (by proper personnel identified per CIP-003 / R2) reviews on a periodic basis (at least annually) of the categorization of BES Subsystems under the entity's ownership. R1.2: add text to require signed and dated (by proper personnel identified per CIP-003 / R2) documentation of all engineering evaluations or other assessment method(s) approved by the RC or RA(?). If an evaluation or assessment was required, include signed and dated (by proper personnel identified per CIP-003 / R2) documentation of the request to and response from the RC or RA(?). 2. The term Reliability Assurer is used in the standard but is not yet an official NERC Glossary Term. It needs to be added to the definitions being proposed. 3. Requirement R1.1 – the list of activities for which an update is required should specifically include when a Responsible Entity is notified of a change per Requirement R2. Similar updates are needed in the Measures section. 4. Requirement R1.1 – replace the word "impact" in line 4 with "categorization". 5. Requirement R1.2 – the expectation that study based assessment methods would be acceptable to classify or change impacts violates a core principle of the activity as stated in the supporting guidance document. Page 4 Paragraph 2 states that the impact "thresholds are defined to provide a straightforward and objective path …to determine impact categorization…" The use of engineering evaluations or other assessments results in a much less objective and potentially inconsistent application of the categorization process, requires a significantly higher level of resource commitment to perform the evaluations, and introduces the need for Reliability Coordination or Reliability Assurer oversight/validation. Further, for some of the impact criteria such as frequency response, sufficient quality models do not exist upon which evaluations could be reliably based to determine system collapse. This significantly undermines the "bright-line" approach intended and therefore is counter to the team's stated goals in this effort. These study-based methods need to be minimized or eliminated and the bright-lines more clearly defined.
Dominion	Disagree	To satisfy CIP-002-4 R1.1, entities will need to know what changes could affect the impact of BES Subsystems on the Bulk Electric System. It can be inferred from this premise that Responsible Entities who possess the capability to determine those changes would have an obligation to identify such changes. The entities with such capability typically consist of one or more of the following: Reliability Coordinator, Balancing Authority, Transmission Operator and/or Regional Entity. Dominion suggests that a requirement be added to ensure that such entities develop appropriate criteria to identify such changes. While Dominion agrees with most portions of requirement R1.2, some modifications are needed. Specifically, Dominion suggests that: 1) Reliability Assurer should either be added to Applicability Section 4.1 or it should be removed from R1.2; and 2) a specific requirement should be added for each Reliability Coordinator or Reliability Assurer to identify their

Organization	Yes or No	Question 4 Comment (Response page 16)
		approved engineering evaluation or other assessment method(s).
Encari	Disagree	We agree in theory with this requirement; however, we express concern over the implementation timetable for any modification of the BES subsystems within an entity. We have encountered many situations that due to system failures associated with Critical Assets that new critical assets are identified. It is very important to handle these BES Subsystem situations associated with unplanned outages.
US ACE – NW	Agree	
SCE	Disagree	This requirement would require constant updates to the list of BES Subsystems by each Responsible Entity, as any change that "could affect" the BES Subsystems would trigger the requirement for an update. It is unclear that any Reliability Coordinator or Reliability Assurer would have the capability to approve all of the types of engineering evaluations or assessments that could be applied to the virtually infinite number of potential changes. A Responsible Entity must have the opportunity to seek up-front confirmation from its respective Reliability Coordinator or Reliability Assurer in order to verify that its classification of BES Subsystems is correct. It is unclear how this would be accomplished under Requirement R1. Further, the phrase "any change in the electrical system" is too broad. The drafting team should classify quantitative metrics for what is "change". The clarification should be such that it can scale across the different entities in the industry and across operational environments.
USBR	Disagree	There are three points, the requirement R 1.2 implies that the Reliability coordinator may approve un- documented assessments. The requirement should indicate that the Responsible Entity shall "provide" approved evaluation or assessments. Second, the requirement should be specific to the attachment sections in which the approval is made. Namely Sections 1.1, 1.5, 2.1,and 2.2. Last, there is not requirement for bilateral communication in assessing the impact of assets or cyber systems with the neighboring interconnected responsible entities.
Dyonyx	Agree	
MISO	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets."
Westar	Disagree	
Green Country	Disagree	I wish I had a suggestion, BUT the terms "under its ownership" are troublesome. The responsible entities have already been defined as result of registration. To prevent future misunderstanding remove that phrase. Because I can see a harsh interpretation of requiring ownership to compile all its owned generation into a combined MW output and then apply

Organization	Yes or No	Question 4 Comment (Response page 16)
		it to table 1 for example
Oregon PUC		The term “engineering evaluation or other assessment method(s)” needs to be better clarified and specified. The standard needs to have clearer and more specific processes for exceptions.
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	PGE does not agree with this requirement. In 1.1, the phrase "or any other change in the electric system that could affect the impact" is very vague and would lead to difficulties in demonstrating compliance on the part of registered entities, and assessing compliance on the part of regulating entities. For example, would this vague definition encompass changes made on neighboring systems because they would “affect the impact” of PGE’s system, therefore triggering the reporting requirement? Such a situation would not only be impossible to demonstrate or assess compliance, but also onerous to attempt to track. In 1.2, based on the structure of the sentence, PGE is unclear whether this means every engineering study or evaluation must be approved and such approval documented, or whether it would require using only methodologies approved by the reliability coordinator.
PSEG	Disagree	Comment #1: Suggested rewrite for Requirement 1: Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…” We suggested in question 1c that the term “BES Subsystem” be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding the SDT expectations. In addition, the term “BES Subsystem” does not align with the terms used in Attachment 1. (Attachment refers to the Generation Subsystem, Transmission Subsystem and Control Center) We believe that the result of this requirement is that each entity has to identify through some naming convention a list of each Generation Subsystem, Transmission Subsystem and Control Centers they own. As we provided under the definition of Transmission Subsystem this will require entities to understand the relationship between their BES Cyber Systems and that could be compromised through the specific BES Cyber System. Examples repeated from Question 1e 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. We believe that our suggestion aligns this requirement to the terms used in Attachment 1. Additional comments about the proposed requirement:

Organization	Yes or No	Question 4 Comment (Response page 16)
		What is the goal of this requirement? and What is the requirement asking of Responsible Entities? Is this requirement requiring an entity to make a summary list of all of our Transmission Subsystems (Substation Names) and identify them as either “High”, “Medium” or “Low”? Or Is this requirement requiring an entity to make a detailed list all of our Transmission Subsystem including its associated Cyber Assets and identify them as either “High”, “Medium” or “Low”? Suggested rewrite for Requirement 1.1: Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. Our proposed goal is clear as to when the update has to occur for big / major changes to an entities system. We believe that the phrase “any other change in the electric system that could affect the impact of BES Subsystems on the BES” should be deleted because it does not provide enough clarity as to what would and would not qualify. As an alternative the SDT should consider adding a new requirement for entities to perform an annual review of its list for those items which an engineering assessment was performed. An annual review would capture the goal of getting entities to review and if necessary update their list based on changes to their system. Suggested rewrite to Requirement 1.2: Replace Reliability Coordinator or Reliability Assurer with Planning Coordinator. We believe that the Planning Coordinator is the best entity to provide review and feedback on engineering assessments.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI’s comments regarding this question. This includes suggested changes to attachment 1. In addition, Wisconsin Electric Power Company feels the 30 day requirement to update is too short and should be extended to quarterly
Idaho Power	Disagree	A more prescriptive description of what an appropriate engineering evaluation or assessment method would be better. As written, the RC will be approving multiple proposals which could lead to inconsistencies in the categorization of subsystems.
SOCO	Disagree	As written, it is not explicitly stated that the listing of cyber systems associated with BES Subsystems listed in R1 is only to be done for the R1 listing for the Entity performing the analysis. This leaves in limbo, for example, the situation where the output from a syncrophasor unit is not used for reliability purposes by an Entity but is used for those purposes by their RTO. The intent that an Entity is only responsible for cyber systems associated with their own BES subsystems should be made explicit. In 1.1, the phrase “any other change in the electric system that could affect the impact” is very nebulous and will be hard

Organization	Yes or No	Question 4 Comment (Response page 16)
		to prove compliance to an auditor if “every modification” isn’t explicitly studied, documented and approved. Approval by a outside party is required under this Requirement for any engineering evaluation. The Standard identifies the reviewing party as the Reliability Coordinator or Reliability Assurer. This may require that utilities evaluate documentation from neighboring competitors. To accomplish this may require a transfer of potential proprietary and competitive information. Further more it would require that security related information be more widely disseminated to individuals outside the security policy and procedural control of the originating organization. This requirement will present staffing, scheduling and budgeting burdens on the reviewing party to perform evaluations for potentially multiple utilities. The use of engineering evaluations is typically auditable but not subject to a routine outside independent review. The Regulator should consider the development of a review body or allow the use of an independent reviewer it this approach becomes a requirement. Engineering evaluations for some entities may require a seal from a registered professional engineer certified in the State of the installation. This may require that the approvers be registered in numerous States. Suggest that the Reliability Coordinator for the balancing authority approve the engineering studies and list of identified assets for their own balancing authority. They are the most knowledgeable of their own system conditions and planning studies and would be in the best position to understand impacts of assets on their system.
DTE	Agree	
AEP	Disagree	Refer to question #2 above.
Edison Mission	Agree	
Calpine	Disagree	New purchased assets may take longer than 30 days to submit a list. We suggest allowing 90 days for new assets.
NS%T	Disagree	We believe impact criteria should be simplified for the sake of inter-Entity and inter-Region consistency. We are concerned about the situation that could arise with sub-requirement 1.2 if a Responsible Entity's assets spanned multiple RCs and the RCs did not agree on the results of engineering evaluations.
Flathead	Disagree	For low impact assets, the 30 day requirement is an unnecessary burden on local distribution entities that currently don't have critical assets, but might under this low impact inclusion. Should be an annual evaluation only. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at LSE/DPs that didn't identify critical assets.
E ON	Disagree	The update should be performed on a by exception basis. In other words, a complete inventorying of all BES Subsystems (high, medium and low) is unnecessary. Only those BES Subsystems that fall into a new category as a result of new or decommissioned facilities should be included in any re-appraisal.
Carthage	Agree	

Organization	Yes or No	Question 4 Comment (Response page 16)
WECC	Disagree	The determination of criticality should not be required to be validated by the RC's or Reliability Assurer. We do not agree that the RCs are equipped or staffed to perform this function.
Entergy	Disagree	1. Beginning the process using R1 & Attachment I is illogical for addressing this cyber security puzzle, and only obfuscates the issues truly salient to the solution set. 2. R1/Attachment I create a great deal of unnecessary ongoing work and regulatory exposure. 3. Clear delineation of exactly what constitutes a "BES Subsystem" in practice in any number of various scenarios is elusive at best. 4. Is it appropriate to require Reliability Coordinators to accept responsibility for 'approving' and/or 'validating' "engineering or other assessment methods?" If the Reliability Coordinator is found to have been mistaken after the fact, who will be fined? What if the mistake involves Entities whose operation spans more than the aegis of an individual Reliability Coordinator? 5. In practical terms, 30 days is a very narrow time window for what's required.
CenterPoint	Disagree	Disagree – See comments on 1.a. Besides the problems with the proposed new "subsystem" approach, it is unrealistic to perform meaningful on-going engineering evaluations or other assessments with each and every change to the BES, which is the de facto R1.1 requirement. It is even less realistic to add a new layer of review to this process on an on-going basis as R1.2 requires. Also, R1.2 would require definition of yet another functional entity, "Reliability Assurer", which will likely cause even more confusion among practitioners trying to implement the new paradigm.
LCRA	Agree	
FRCC	Disagree	In requirement 1.1, the phrase " or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System" is extremely broad and could be almost anything. This would most likely lead to an interpretation request which should be avoided in the development of the requirement. If the drafting team knows what kind of changes would fall in this category they should consider specifically stating them or need to revise to remove the ambiguity in the phrase.
NIPSCO	Disagree	We are concerned with the ability of the RC or the RA to make the determination required in 1.2. Additionally, we would like clarification regarding what the RC or RA is approving; the methodology, the HML categorization of the BES subsystems, or both. Suggestion: Review and discuss with the RC's and RA's their position on satisfying this requirement as written. Additionally, clarify the intent of the required RC / RA approval.
ConEd	Agree	
EEI	Disagree	1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the

Organization	Yes or No	Question 4 Comment (Response page 16)
		Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability "must run" units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem. 1.5. Each Transmission Subsystem that contains substations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station. 1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) consistent with FAC-10. 1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We believe that 1.9 is duplicative with the presence of 1.1-1.4 and 1.8 We believe that 1.10-1.12 is duplicative with the presence of 1.7 1.13. Each Protection System associated with Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an material adverse reliability impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more …… * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and

Organization	Yes or No	Question 4 Comment (Response page 16)
		that functional entity submits a written request for the information. If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments. ... 2. BES subsystem with the following characteristics will be determined to be Medium Impact (M) unless it has been determined that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 1,000 MVA or more. 2.2. Each Transmission Subsystem that contains substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency stability support. 2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. 2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. 2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above. Regarding 1.1, additional clarity is required. A literal reading of 1.1 could require an entity to update its categorized list of BES Subsystems, if there is any change by any entity anywhere on the grid. This could include changes to the grid brought by natural disasters such as ice storms or hurricanes. Consider: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the Responsible Entity commissioning new BES Subsystem(s), decommissioning BES Subsystem(s) or being notified by a transmission planning authority of changes in the electric system that could affect the impact of the Responsible Entity's BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.

Organization	Yes or No	Question 4 Comment (Response page 16)
		Regarding 1.2, the industry would be aided by the provision of examples of approved engineering evaluation methods. EEI believes that the standard should either better define an acceptable/minimum engineering evaluation that needs to be performed or specify the ability of individual entities to determine they are allowed to determine the engineering evaluation that they will perform. If the standard is going to specify external review they need to provide some guidance on what the level of review is going to be and the items that need to be considered for the review. EEI is concerned about the designation of Reliability Coordinator or Reliability Assurer as being responsible for this oversight role. The Reliability Coordinator or Reliability Assurer may not have sufficient resources or expertise to satisfy the obligation. It may be more appropriate for the Planning Coordinator and Transmission Planner to perform this task, subject to review.
O&R	Agree	
Alliant	Disagree	R1 needs clarity concerning joint ownership and should be rewritten as follows: " Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 - Criteria for BES Impact Categorization of BES Subsystems. R1.1 needs clarity and should be rewritten as follows: "The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of its commissioning of any new BES Subsystem, its decommissioning of any existing BES Subsystem or its modification of any existing BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days following the completion of the commissioning, decommissioning, or modification. The term "Reliability Assurer" needs to be defined in the NERC Glossary of Terms.
Ameren	Disagree	Ameren feels that 30 days is too short of time to update the categorized list of BES Subsystems, 90 days would be much more practical. In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved. Requirement R1.2 should be tied to testing of extreme contingencies, such as those described in TPL-004-0. Also, we disagree with the role of Reliability Coordinator as the RC has a time horizon too short for this task per the NERC Functional Model. For this reason, replace Reliability Coordinator with Planning Authority who would work with the Transmission Planner. Also, the role of the Planning Authority should be that of inclusion of additional assets not in evaluation in assessment methodology per the FERC order 706, par 325.
Black Hills	Disagree	Agreement is conditional upon thorough understanding of "ownership". Joint ownership requires understanding who assesses, and if multiply "assessed" whose view prevails. Under CIP-002-1, if two entities jointly owning as asset disagree on criticality, the owner designating as 'critical' prevails. In 1.2, does RC or Regional Assurer approval of assessment method(s) used by the Responsible Entity refer to "approval of the general process" or a specific assessment approval? Further, do both 'evaluations' and 'other 'assessment methods' need to be approved; or just 'other

Organization	Yes or No	Question 4 Comment (Response page 16)
		assessment method(s)'?
TNMP	Disagree	TNMP believes the phrase "BES Subsystems under its ownership." does not handle jointly-owned facilities well. Consider the scenario where Responsible Entity 'A' has ownership of 4 breakers and two lines coming into a substation with an operation voltage greater than 300kV and Responsible Entity 'B' owns eight additional breakers and four additional lines to the same substation at the same rating. The two Entities separately-owned BES Subsystems are connected by the substation bus. If all the controls for the substation come into a single control house owned by Responsible Entity 'B', and the whole station is controlled by Responsible Entity 'B' should Responsible Entity 'A' be responsible for control house equipment as a result of its ownership of the devices? Another variation on the scenario is each Responsible Entity owning a separate control house for each part that they own and control. Using the criteria in CIP-002 Attachment 1, does Responsible Entity 'A' have a BES Subsystem with High or Med BES Impact? The piece Responsible Entity 'A' owns only has two transmission lines and two pieces of bus connecting to piece owned Responsible Entity 'B'. However, the substation as a whole has 6 lines at a voltage level greater than 300 kV. While this second scenario deals more with the content of CIP-002 Attachment 1, it is still an issue that should be resolved in either the wording of Requirement 1 or Attachment 1. Another concern with the proposed requirement is the "or any other change in the electric system that could affect the impact of BES Subsystems" statement. If a change occurred in the system of Responsible Entity 'A' that altered the impact on a BES Subsystem in the connected system of Responsible Entity 'B' then 'B' would be liable for the 30 calendar day clock. Requirement R2 puts the onus upon the Responsible Entity owning a Generation Subsystem to provide information to connected Responsible Entities, which may not have access to the same information. The current wording of R1 puts the onus upon the Responsible Entity who doesn't have the information to know about the information. In the scenario if Responsible Entity 'A' was to report the change to its Reliability Coordinator or Reliability Assurer then it should be up to the Reliability Coordinator or Reliability Assurer to notify Responsible Entity 'B' that a neighboring change has impacted one or more Transmission Subsystems of Responsible Entity 'B'.
NVEnergy	Disagree	We agree with the concept of the requirement, yet are concerned about two things: the lack of definition round what sort of "other change" that "could affect" the impact on the BES as indicated in 1.1 and the discretion allowed to the Entity to conduct the engineering evaluation or assessment provided in 1.2. It is not clear that the Reliability Coordinator is in the best position to approve that method without having clear guidance and boundaries to promote consistent approaches. While the SDT's efforts appear to attempt to bring some clarity to the characteristics that define the Impact Level (High, Medium, Low), this effort is then unraveled by allowing for an undefined alternative engineering analysis to overturn the initial classification. This would be acceptable if more guidance is provided, perhaps via another attachment, to help the Entities conduct consistent exclusion analyses. We believe there should be more focus placed on the cyber systems themselves, which on an individual basis can impact the BES.
MWDSC	Disagree	Unclear what assessment method will be approved. Recommend having a guideline at the same time as standard is completed such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009. Recommend changing 1.2 to: "The Responsible Entity shall document any engineering evaluation, or in the alternative another assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to

Organization	Yes or No	Question 4 Comment (Response page 16)
		support the categorization of BES Subsystems where required by Attachment 1." Also, make similar change to M1.2 and Attachments 1.5 and 2.2.
Empire	Disagree	I disagree with the 30 day requirement specified in 1.1. This should be extended to 120 days due to the complexity of these devices and the approvals that could be needed to make these changes.
SWTC	Agree	
SCEG	Agree	
Exelon	Disagree	We are concerned that statement in 1.1 is currently open for inconsistent interpretation and suggest the following revision: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change made by the Responsible Entity that could affect the categorization of the BES Subsystem, within 30 calendar days of the completion of the change. We would ask for more clarification concerning “engineering evaluation” as stated in section 1.2. Specifically the criteria and basis to be used, and to address the possibility that “Responsible Entity” and Reliability Coordinator/Reliability Assurer may for some entities be one and the same.
BPA Trans	Disagree	1) There appears to be a void in CIP-002-4. Although stated in the purpose statement, there is no actual requirement statement that the Responsible Entity identify and list their BES Subsystems. CIP-002-4 only requires that those systems be categorized. It seems to assume that identification and listing of the “BES Systems under its ownership” has already occurred. This may not be a big point. However, the original CIP Standards were specific about this part of the process. Note: The guidance document dated December 2009 states that Step 1 of the process is to perform a BES Subsystem Inventory. It continues that “The inventory of BES Subsystems …”and “The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design…….” indicating that an inventory of BES Subsystems is necessary. We believe that the first requirement of CIP-002-4 should be the initial identification of BES Subsystems with the appropriate stated criteria/functions etc. Starting the CIP with a requirement to “categorize” assumes that the Subsystems themselves have already been identified. The text provided below is suggested as an example of a potential new R1 to “inventory/identify” BES Subsystems. R1. The Responsible Entity shall create an inventory of all BES subsystems owned by the entity, including all: Generation Subsystems, Transmission Subsystems, and Control Centers. R1.1 The Responsible Entity shall base its inventory on the list of Functions Critical to the Reliable Operation of the Bulk electric System (CIP-002-4 Attachment 2) R1.2 The Responsible Entity should consider any associated BES Cyber Systems when performing the inventory and

Organization	Yes or No	Question 4 Comment (Response page 16)
		defining the boundaries of BES Subsystems. Note: R1.1 and R1.2 are taken directly from the December 2009 guidance document. With the addition of new requirement #1, existing R1 becomes R2. It is edited for clarity: R2. The Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. (Violation Risk Factor: High) R2.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. R2.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1. Additionally, no criteria is provided for the identification of BES Subsystems other than “Generation Subsystems, Transmission Subsystems and Control Center.” Are there others?
HQT	Disagree	RC should be removed from 1.2.
Allegheny Energy	Agree	We support requirement 1.1 as it is an extension of the current CIP-002 version 1. We are concerned with the ability of the Reliability Coordinator to make the determination required in 1.2.
KCPL	Disagree	I am concerned regarding the potential flood of requests to the Reliability Coordinator(s) that could result from Requirement 1.2 with the criteria proposed here under Attachments 1 and 2. I believe appropriate criteria may substantially stem requests to the RC.
Connectiv Energy	Agree	
MidAmerican	Disagree	CIP-002-4 as proposed requires all BES facilities to be in CIP scope. It thereby addresses the criticism that entities did not include enough facilities. MidAmerican supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all operated BES facilities: transmission substations and generation resources connected at 100 kV and above and transmission control centers that are subject to other existing NERC standards. This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards.

Organization	Yes or No	Question 4 Comment (Response page 16)
		However, categorization level determinations should be addressed in the security control standards. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. Further, if engineering evaluations are required in some cases as drafted in CIP-002-4, the prescription to update documentation within 30 days of a change in the BES is not realistic.
CPG	Disagree	R1.1 would require monthly reviews of all assets to ensure that no changes have been made, and that if there were any changes, they would have to be documented. Changing this requirement to quarterly reviews would allow for a more thorough investigation of any changes and allow time for those changes to be well documented. R1.2 would require the Reliability Coordinator to approve all engineering evaluations (or other methods) to support the categorization of BES Subsystems. If a Generator Owner/Operator concurs with engineering assessments shared with its connected Transmission Owner/Operator, then that assessment would ensure proper coordination and categorization of BES Subsystems. Having it then approved by the Reliability Coordinator adds another cumbersome and unnecessary level of approval. A definition or clarification as to what is meant by the "Reliability Assurer" is also needed.
Santee Cooper	Disagree	Still do not believe the BES Subsystem classification is clear in achieving the overall objective of the new Standard.
OGE	Disagree	• Should dual-ownership of BES subsystems be addressed in this document? • The phrase "any other change in the electric system that could affect the impact…" is excessively open-ended. Needs to be a change that could increase the impact rating. • Is 1.2 indicating that the RE shall have the RC approve their engineering evaluation and/or assessment method(s) or should the RE document that it is using an RC approved engineering evaluation and/or assessment method(s)?- • SDT should extend the time period for updating the list and ultimately asset compliance to 90 days or greater.
Oncor	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose the following: Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems.
PPL Supply	Disagree	A more precise definition of Black Start generating units is needed that in the proposed Rev. 4 or the EEI comments. To say that "Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem." is inadequate to identify only those generating units that are used for initial restoration of the BES. System restoration plans normally identify all units from the blackstart initiating through the thermal generation at the end of the cranking path, including any intermediary units, so clarification is needed to avoid

Organization	Yes or No	Question 4 Comment (Response page 16)
		misinterpretation.
St. George	Agree	
NGRID	Disagree	The use of "BES Subsystems" is not consistent with the terms used in Attachment 1 and should be replaced by the specific terms such as Transmission/ Generation subsystems.
MGE	Disagree	Do not agree with the following: The BES Subsystem definition is not required and should be removed since Generation Subsystem, Transmission Subsystem, and Control Center are clearly defined. R1, "As a step in identifying appropriate security controls for its assets" should be deleted; the statement does not add content or instruction to the requirement. R1.1, "or any other change in the electric system" should be removed because it does not provide enough clarity and could be interpreted to mean just about anything. R1.2, Reliability Assurer is not defined by NERC. Please provide a definition. And it is not listed in the Applicability section, please add. R1.2, As written the RC or RA (?) will have to approve all engineering evaluations or other assessment methods to support categorization of BES Subsystems where required by Attachment 1. What is the basis of electing the RC or RA to have the authority to approve a methodology concerning a BES Subsystem of an entity other than that entity? To reduce any risk associated with categorizing of a BES Subsystem, the RC or RA will simple not approve any type of evaluation, ever. There are no other requirements or proposed guide lines to assist in the evaluation that the RC or RA will use in approving the categorization of BES Subsystems. Order 706 paragraph 325 states "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets." If this was added to reduce what we now know as TFE's, it does not. Paragraph continues with "We recognize, however, that there may be a legitimate reason for a responsible entity to dispute such a determination, possibly through an appeal. We leave it to the ERO to determine the need for such an appeal mechanism and, if appropriate, the development of appropriate procedures (or reliance on appeal procedures currently provided in the NERC Rules of Procedure). While the ERO may determine that an appeals process is a necessary aspect of this program, we do not believe that the burden of such appeals outweighs the benefits of the external review of critical asset lists". Recommend R1.2 be deleted in its entirety.
FE	Disagree	In general we do not support the categorization described by the R1 and Attachment 1 as described in our prior comments. However, we offer the following comments: 1. Item 1.1: The team should consider a separate requirement for this such that a Lower VRF can be applied. Merely updating a list within 30 days is a documentation item that should not be subject to a High VRF penalty.

Organization	Yes or No	Question 4 Comment (Response page 16)
		2. Item 1.2: FE believes that the need for RC or RA approval can be avoided by requiring the study follow the PC's Methodology for identifying IROL as defined in FAC-010/FAC-014. Furthermore, we do not support the use of the RA. The RA is a Functional Model Guideline (which we did not support) and the NERC registration criteria for responsible entities do not support the RA classification.
TECO	Disagree	Reliability Assurer is capitalized but not otherwise defined. Reliability Assurer does not appear in the FERC approved Glossary of Terms nor in the Functional Model. This position is unclear and should be removed. We support the EEI comments regarding attachment 1 and offer additional clarification for items 1.2, 1.4 and 2.2. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of either the Responsible Entity's Contingency Reserve obligation or if the Entity is part of a Reserve Sharing Group, the Reserve Sharing Group's Contingency Reserve obligation. 1.4. Each Transmission Subsystem comprising the Cranking Paths and each Blackstart Generation Subsystem that has been included in the regional system restoration plan. 2.2. Each Transmission Subsystem that contains substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines connected to the station.
CECD	Disagree	1. "As a step in identifying appropriate security controls for its assets" should be deleted because the Purpose of the standard has already been stated. 2. What qualifies as an engineering evaluation? (3) The requirement should explicitly indicate that a dated list and categorization of BES subsystems is necessary for compliance as indicated in the relevant measurement.
MRO	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose the following: Each Responsible Entity shall categorize the BES Subsystems it operates by applying the criteria in CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems. We feel R1.1 is ambiguous as written, and would propose the following: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of its commissioning of any new BES Subsystem, its decommissioning of any existing BES Subsystem or its modification of any existing BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days following the completion of the commissioning, decommissioning, or modification. We also feel the term "Reliability Assurer" should be defined in the NERC Glossary of Terms.
GTC	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing "within 30 calendar days of the completion of the change" with "within 30 calendar days of the Responsible Entity becoming aware that the change has occurred". Also, to clarify applicability, we suggest

Organization	Yes or No	Question 4 Comment (Response page 16)
		replacing the phrase "that could affect the impact of BES Subsystems" with "that could affect the degree of impact of the Responsible Entity's BES Subsystems." For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
Xcel	Disagree	We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. We believe 30 days is too short and suggest 90 days is more appropriate.
BGE	Disagree	We do not agree with this requirement and suggest changes to Attachment 1 as detailed in our response to Item #3. The exact start time for the 30 day clock needs clarification. Work could be completed in stages, for example: BES Subsystem work may incorporate new equipment brought on-line in stages. Is the "completion of the change" defined as completion of each individual stage or the entire project? Particularly important, is the relationship of system protection work to the completion of the entire project, that is, system protection work may be completed and in service before equipment is energized. The term "Reliability Assurer" needs to be fully defined. According to the NERC "Reliability Functional Model Technical Document", version 5, December 2009, the specific role of the Reliability Assurer is not fully developed at the present time. The approval criteria used by the Reliability Coordinator or Reliability Assurer is not defined.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Has the drafting team coordinated with all registered Reliability Coordinators (RC)on how they will handle this? Or confirmed that they are ready to handle these requests? Also, who would be the Reliability Assurer (RA)? This does appear to be a FERC approved registration criteria yet. The role of the RA in Version 4 of CIP-002 is critical, there should be a better understanding of who or what type of organization will perform this activity. Also, in the provision that either the Reliability Assurer or the Reliability Coordinator may approve the engineering assessment as stipulated in Requirement 1.2, there should only be one option either the RA or the RC but not both. We feel that the drafting team needs to coordinate with all of the registered Reliability Coordinators and/or their agents to confirm that they are prepared to handle requests for validating engineering assessments. There should be language within the standard that holds the RC to be required to perform this task from a mandatory compliance standpoint.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP suggested in question 1c that the term "BES Subsystem" be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding of the SDT expectations. In addition, the

Organization	Yes or No	Question 4 Comment (Response page 16)
		term “BES Subsystem” does not align with the terms used in Attachment 1.
FMPA	Disagree	As described earlier, the addition of the concept of Subsystem is unnecessary and adds ambiguity and complexity. The requirement would be much improved by simply replacing Subsystem with Cyber System. Bullet 1.1 could be modified to include commissioning or decommissioning of any Facility or BES Cyber System. Also, the use of the term “assets” adds ambiguity. The only security controls envisioned are for Cyber Systems, so, use the term Cyber Systems.
Duke	Disagree	We disagree with the approach of categorizing BES Subsystems and instead prefer the alternative “Cyber First” approach. Also, we disagree with making the Reliability Coordinator responsible for approving engineering or other assessment methods used to categorize BES Subsystems, because the Reliability Coordinator does not have this capability or resources.
NBSO	Disagree	1.2 is not clear. Attachment 1 should allow for more stringent RC input. The RC should not be used for entities to get exemptions from high impact level.
AESI	Disagree	The impact of a BES Subsystem may be affected by changes external to the Responsible Entity. As a result, the Responsible Entity may not be aware of such changes and may not be able to update its list of BES Subsystems in a timely manner. We suggest replacing “within 30 calendar days of the completion of the change” with “within 30 calendar days of the Responsible Entity becoming aware that the change has occurred”. Also, to clarify applicability, we suggest replacing the phrase “that could affect the impact of BES Subsystems” with “that could affect the degree of impact of the Responsible Entity’s BES Subsystems.” For Requirement 1.2 to be practical, some process must be in place for Responsible Entities to submit engineering evaluations/assessment methods to Reliability Coordinators/Reliability Assurers in order to have them approved in a timely manner. We are not aware of any such process being mandated by NERC. As a result it may be difficult and/or time consuming for an entity to have their assessment methods approved.
IESO	Disagree	In concurrence with the IRC we submit the same response as follows: At the CIP-002-4 Webinar, the Standard Drafting Team invited comments/suggestions on how best to address “third party review”, as is required by Order No. 706 (and 706-A). See Presentation at Slide 10. We appreciate the SDT inviting comments on other approaches to addressing Order No. 706’s requirement that there be some external-party review of Responsible Entity’s lists of those assets designated as critical, and potentially requiring critical infrastructure protections. In its presentation, the SDT discussed the need to respond to Paragraph 322 in Order No. 706; the comments below discuss Paragraph 322 and other relevant paragraphs in Order No. 706 and 706-A. These comments also pertain primarily to the US-based registered entities, because some Canadian Entities have different oversight authority/enforcement responsibility than their US-based counterparts. First, and foremost, the matter of third-party review should be handled through the NERC Rules of Procedure/CMEP, and not in the Standard Requirements. The key parts of Order No. 706 (and 706-A) set out three (3) principles.

Organization	Yes or No	Question 4 Comment (Response page 16)
		(II) Responsible entities are, and should remain, responsible for identifying their own assets as requiring critical infrastructure protection. The SDT makes clear in the plain language of the Standard that Responsible Entities are responsible for their own assets. Paragraph 328 of Order No. 706 states that: "responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large – in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility." See also Order No. 706-A at P53 (: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity. The fact that the Commission has directed the ERO to develop an external review process – as a backup to help assure that the responsible entity does not overlook any critical assets – does not shift this responsibility from the responsible entity to whatever entity conducts the external review.") (III) NERC and the Regions should issue guidance to Responsible Entities that do not have a "wide-area" view in order to assist them in identifying which of their assets required critical infrastructure protection (Order No. 706 at P322). The SDT had provided guidance in the form of the Standard itself – i.e., Attachment 1. This Draft Standard effectively directs Registered Entities on how to classify their assets. (IV) External review is necessary to: (a) help identify trends in the industry (Order No. 706 at P322 and to support consistency (Id.), and is necessary to review asset more frequently than would occur through the regular audit cycle. (Order No. 706 at P324) (FERC "does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations"). With regard to Principle III, FERC explained that NERC may choose to "designate" a Registered Entities (such as, but not necessarily, a Reliability Coordinator) as responsible for this external review if NERC/Regional Entities determined that they did not have the resources/expertise to conduct this review. (Order No. 706 at P255)("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). In Order No. 706-A, FERC added that if NERC designated a Reliability Coordinator as having oversight/review authority, the Reliability Coordinator should have the same liability protections as NERC. (Order No. 706-A at P53).

Organization	Yes or No	Question 4 Comment (Response page 16)
		In drafting CIP-002-4, the SDT therefore largely adhered to the first two principles. The draft language in R1.2 confuses the Principle III, and therefore takes a wrong approach to addressing the Commission's concerns in Order No. 706. With regard to Principle III, the need for more frequent external review than that provided by audits can and should be handled outside of the Standard Development Process. For example, NERC and the Regions can establish spot-checks or off-site audits through the CMEP program, and NERC can require Responsible Entities to submit information to it (or the Regions) through an information request developed under its Rules of Procedure. If the SDT and NERC address the role of third party review through NERC's administration of its Rules of Procedures, many significant problems with R1.2 would be eliminated. These problems are summarized below. First, because NERC would register Regional Entities as "Reliability Assurers", the manner in which Regional Entities would carry out its oversight task should be handled through NERC/FERC review or audit of Regional Entities' adherence to their Delegation Agreements. This would be a better approach to checking on the Regional Entities' performance in providing external review then through an Enforcement Audit process. Second, it is premature to place "Reliability Coordinators" in the Standard. Because NERC has not found that it lacks sufficient resources to take on the external review responsibility, and thereby has not "designated" any other type of Registered Entity with this responsibility, it is premature for the Standard to make reference to the Reliability Coordinator. See Order No. 706 at P255 ("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). If the Standard Drafting Team is committed to including in its Standard reference to a Registered Entity as having external review oversight, it should wait until NERC makes its designation. Third, assigning external review responsibilities to the Regional Entities (as Reliability Assurers) would facilitate achieving FERC's goal of consistency. Because NERC and the Regional Entities work closely as part of their Regional Entity Delegation Agreement, and because there are fewer Regional Entities than Reliability Coordinators, achieving consistency will be easier if the Reliability Assurers (i.e., Regional Entities) have the external oversight responsibility. Fourth, even if NERC "designates" a Registered Entity (such as, perhaps, a Reliability Coordinator) as having a role in providing external review, the Registered Entity would have the same liability protections as NERC, the Registered Entity is essentially carrying out this role as a NERC-designee. It is easier to capture the roles, responsibilities and liabilities protections through amendment to the Delegation Agreements and Rules of Procedure. In Order No. 706-A, FERC reaffirmed the protections given to external reviewers. See Order No. 706-A at P53 (""we agree [with the ISO/RTO Council] that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself."). These protections include no finding of liability unless intentional misconduct or gross negligence is found. See, e.g., Bylaws at Section 3 (NERC's trustees, officers, employees, and agents are held harmless "for any injury or

Organization	Yes or No	Question 4 Comment (Response page 16)
		damage to [any NERC Member] caused by any act or omission of any trustee, officer, employee, agent, or volunteer in the course of performance of his or her duties on behalf of the Corporation, other than for acts of gross negligence, intentional misconduct, or a breach of confidentiality”). Fifth, the combination of R.1.2 and 1.1. and 1.5 in Attachment 1 appears to require an external review by the Reliability Assurer or Reliability Coordinator to exclude assets. This exclusion is contrary to the type of external review identified in Paragraph 325 of Order 706. “However, an external reviewer’s role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.” Clearly the Commission intended to add facilities to the critical assets not exclude them with the external review. R1.2 does not explicitly describe the nature of the third party review, we interpret the Draft Requirement to not require a Reliability Coordinator/Reliability Assurer to conduct such reviews and/or issue approvals. Clarity could be useful, because others interpret the Standard to require an exception-type external review – i.e., when a Registered Entity does an engineering evaluation that claims that its assets should be classified according to Attachment 1. Others have interpreted the language to require external review of all entities to determine whether they are leaving out assets from their lists. Sixth, even if the R1.2 is meant only to apply to an external reviewer doing “exception-type” reviews, including this role in the Standards suggests that so long as a Responsible Entity does any type of engineering evaluation, the Responsible Entity can effectively shift responsibility to the external reviewer. Because there is no sanction for incomplete or non-substantive evaluations, the External Reviewers may be deluged with requests to “exempt” assets from the Attachment 1 categorization. This language would effectively undermine FERC’s direction that Responsible Entities remain responsible for classifying their assets and they cannot shift this responsible to the Regional Entity or another Organization. See Order No. 706 at P328. In sum, the SRC recognizes that a different set of expectations may apply to those Regional Entities that are also Reliability Coordinators (e.g., WECC). These entities already have liability protections per their NERC delegation agreements, and in their role as Regional Entities, they ultimately have authority over whether the Responsible Entity has correctly identified bulk power system assets as subject to critical infrastructure protection. Similarly, some of the Canadian Reliability Coordinators (e.g., IESO through its enforcement group) exercise similar oversight authority as a Regional Entity with regard to other Registered Entities. While we don’t think the nature of this third-party review should be discussed in the standard itself, if the SDT wants to continue to refer to it in the Standard, at this point, the Standard should only refer to Reliability Assurers.
Manitoba 2	Disagree	What is the purpose of this requirement? Does it imply that the security controls are in place and this is just final documentation? If so, there should be separate requirements with different VRFs (low for the paperwork). Completing the implementation of the security controls would be a High VRF. Please define “any other change in the electric system” as it applies in this definition. Does this scope include the entire electric system across the continent, across the region, or across the Responsible Entity’s territory?

Organization	Yes or No	Question 4 Comment (Response page 16)
		Please define what is meant by "completion of the change" as it applies to this definition. The statement " … affect the impact of the BES Subsystem …" should be revised to "… change the impact categorization level of the BES Subsystem…", which requires the documentation to reflect the changes in categorization, not all the changes in the electric system. We do not feel that 3rd party oversight or approval is required, since the Responsible Entity is responsible for conducting its engineering evaluation with due diligence. The direction of the standard, to include all BES Cyber Systems in the categorization, will mean that security controls will be specified for BES Cyber Systems with a categorization of low. Any such identified security controls will then also be auditable. All BES Cyber Systems are not critical to support a BES Subsystem, and as such should not require auditable security controls. Guidance provided to industry on security controls for low impact BES Cyber Systems would be sufficient for the necessary strategic direction and would not require external audit of these low impact security controls. Low impact BES Cyber Systems should not be listed or be required to be auditable in the standard. Including the low impact BES Cyber Systems will significantly increase the implementation timeframe, increase the cost and will divert resources required to implement the controls associated higher impact levels. Auditable security controls in CIP-003 through CIP-009 should only be applied to high impact and medium impact BES Cyber Subsystems.
ATC	Disagree	Suggested rewrite for Requirement 1: Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…" ATC suggested in question 1c that the term "BES Subsystem" be deleted because the terms Generation Subsystem, Transmission Subsystem and Control Centers provide a clear understanding the SDT expectations. In addition, the term "BES Subsystem" does not align with the terms used in Attachment 1. (Attachment refers to the Generation Subsystem, Transmission Subsystem and Control Center) We believe that the result of this requirement is that each entity has to identify through some naming convention a list of each Generation Subsystem, Transmission Subsystem and Control Centers they own. As we provided under the definition of Transmission Subsystem this will require entities to understand the relationship between their BES Cyber Systems and that could be compromised through the specific BES Cyber System. Examples repeated from Question 1e 1. A substation which contains two separate BES Cyber Systems will have two associated Transmission Subsystem. 2. Two or more substations which use a single BES Cyber System will be identified as a single Transmission Subsystem. We believe that our suggestion aligns this requirement to the terms used in Attachment 1.

Organization	Yes or No	Question 4 Comment (Response page 16)
		Additional comments about the proposed requirement: What is the goal of this requirement? and What is the requirement asking of Responsible Entities? Is this requirement requiring an entity to make a summary list of all of our Transmission Subsystems (Substation Names) and identify them as either “High”, “Medium” or “Low”? Or Is this requirement requiring an entity to make a detailed list all of our Transmission Subsystem including its associated Cyber Assets and identify them as either “High”, “Medium” or “Low”? Suggested rewrite for Requirement 1.1: Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. Our proposed goal is clear as to when the update has to occur for big / major changes to an entities system. ATC believes that the phrase “any other change in the electric system that could affect the impact of BES Subsystems on the BES” should be deleted because it does not provide enough clarity as to what would and would not qualify. As an alternative the SDT should consider adding a new requirement for entities to perform an annual review of its list for those items which an engineering assessment was performed. An annual review would capture the goal of getting entities to review and if necessary update their list based on changes to their system. Suggested rewrite to Requirement 1.2: Replace Reliability Coordinator or Reliability Assurer with Planning Coordinator. ATC believes that the Planning Coordinator is the best entity to provide review and feedback on engineering assessments.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 4 Comment (Response page 16)</th></tr>
<tr><td></td><td></td><td>appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>It is unclear what "appropriate" means. There should be care in adding descriptive words that are open to interpretation and for which no specificity is provided.

R1.1 requires that the categorization must be updated when “….any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System. However it is unclear whether these are permanent changes or could include temporary changes such as extended outages. It is also unclear whether changes caused by adjacent interconnections that could affect the impact of another’s BES Subsystem are included in this requirement. Because of</td></tr>
</table>

Organization	Yes or No	Question 4 Comment (Response page 16)
		these concerns the updated within 30 days may be too short. It is unclear what criteria the RC or RA will use in approving an assessment method in order to ensure consistency as well as timeliness. Puget Sound Energy strongly supports the language defined by EEI in response to this question. Relative to Attachment 1 it is unclear what is the technical justification for using 2,000 MW and 1,000 MW for thresholds of high and medium.
IMPA	Disagree	IMPA recommends changing “ownership” to “operation”. In 1.1, IMPA recommends changing the time from 30 calendar days to 60 calendar days to allow utilities more time. The usage of “any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System” is ambiguous and subjective. IMPA recommends using the words “any change in the BES Subsystem that could affect the impact of BES Subsystems on the Bulk Electric System”. For 1.2, a standard engineering evaluation or other asset method should be developed so the Reliability Coordinators or Reliability Assurers across the country can be consistent or at the very least the regional engineering evaluations should be consistent. In addition, IMPA believes that performing an engineering evaluation or other asset method could be a financial burden on smaller entities that do not have the in-house expertise to perform these evaluations. Therefore, IMPA would like the SDT to consider the use of the prevailing practices of utilities in the region who have performed the engineering evaluations to support the categorization as an acceptable alternative.
ERCOT	Disagree	ERCOT ISO supports Midwest ISO and ISO-NE comments. Further, it would be necessary for a Reliability Coordinator to have a guarantee of safe harbor and indemnity on approval of evaluations and assessments. It should be made clear that the categorization and subsequent protection of assets is the sole responsibility of the asset owner. That responsibility should not ever be abrogated to any other party. Midwest ISO Comments: We disagree with a Reliability Coordinator being drawn into the standard to evaluate an attempt to exclude a facility from compliance with the standards. The simple solution for the Reliability Coordinator to reduce its risk with such a requirement is to not approve the engineering evaluation. We believe that is ultimately what will happen. Furthermore, per Paragraph 325 of Order 706, it is clear the Commission intended to add facilities to the critical assets not exclude them. This requirement is in direct conflict with that intent. Here is an excerpt of Paragraph 325 of Order 706. “However, an external reviewer’s role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets.”
PacifiCorp	Disagree	- CIP-002-4 as proposed requires all BES facilities to be considered as part of the CIP requirements. It thereby addresses the criticism that entities did not include enough facilities. PacifiCorp supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all operated BES facilities.

Organization	Yes or No	Question 4 Comment (Response page 16)
		- This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards. However, categorization level determinations should be addressed in the security control standards. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, PacifiCorp proposes that the development of Attachment 1's concepts be concurrent with the security controls work. - Further, if engineering evaluations are required in order to categorize all BES Subsystems, the requirement to update documentation within 30 days of any changes to any BES Subsystem is not realistic.
IRC	Disagree	At the CIP-002-4 Webinar, the Standard Drafting Team invited comments/suggestions on how best to address "third party review", as is required by Order No. 706 (and 706-A). See Presentation at Slide 10. We appreciate the SDT inviting comments on other approaches to addressing Order No. 706's requirement that there be some external-party review of Responsible Entity's lists of those assets designated as critical, and potentially requiring critical infrastructure protections. In its presentation, the SDT discussed the need to respond to Paragraph 322 in Order No. 706; the comments below discuss Paragraph 322 and other relevant paragraphs in Order No. 706 and 706-A. These comments also pertain primarily to the US-based registered entities, because some Canadian Entities have different oversight authority/enforcement responsibility than their US-based counterparts. First, and foremost, the matter of third-party review should be handled through the NERC Rules of Procedure/CMEP, and not in the Standard Requirements. The key parts of Order No. 706 (and 706-A) set out three (3) principles. (I) Responsible entities are, and should remain, responsible for identifying their own assets as requiring critical infrastructure protection. The SDT makes clear in the plain language of the Standard that Responsible Entities are responsible for their own assets. Paragraph 328 of Order No. 706 states that: "responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large – in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility." See also Order No. 706-A at P53 (: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity. The fact

Organization	Yes or No	Question 4 Comment (Response page 16)
		that the Commission has directed the ERO to develop an external review process – as a backup to help assure that the responsible entity does not overlook any critical assets – does not shift this responsibility from the responsible entity to whatever entity conducts the external review.”) (II) NERC and the Regions should issue guidance to Responsible Entities that do not have a “wide-area” view in order to assist them in identifying which of their assets required critical infrastructure protection (Order No. 706 at P322). The SDT had provided guidance in the form of the Standard itself – i.e., Attachment 1. This Draft Standard effectively directs Registered Entities on how to classify their assets. (III) External review is necessary to: (a) help identify trends in the industry (Order No. 706 at P322 and to support consistency (Id.), and is necessary to review asset more frequently than would occur through the regular audit cycle. (Order No. 706 at P324) (FERC “does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations”). With regard to Principle III, FERC explained that NERC may choose to “designate” a Registered Entities (such as, but not necessarily, a Reliability Coordinator) as responsible for this external review if NERC/Regional Entities determined that they did not have the resources/expertise to conduct this review. (Order No. 706 at P255)(“[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO’s concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System”). In Order No. 706-A, FERC added that if NERC designated a Reliability Coordinator as having oversight/review authority, the Reliability Coordinator should have the same liability protections as NERC. (Order No. 706-A at P53). In drafting CIP-002-4, the SDT therefore largely adhered to the first two principles. The draft language in R1.2 confuses the Principle III, and therefore takes a wrong approach to addressing the Commission’s concerns in Order No. 706. With regard to Principle III, the need for more frequent external review than that provided by audits can and should be handled outside of the Standard Development Process. For example, NERC and the Regions can establish spot-checks or off-site audits through the CMEP program, and NERC can require Responsible Entities to submit information to it (or the Regions) through an information request developed under its Rules of Procedure. If the SDT and NERC address the role of third party review through NERC’s administration of its Rules of Procedures, many significant problems with R1.2 would be eliminated. These problems are summarized below. First, because NERC would register Regional Entities as “Reliability Assurers”, the manner in which Regional Entities would carry out its oversight task should be handled through NERC/FERC review or audit of Regional Entities’ adherence to their Delegation Agreements. This would be a better approach to checking on the Regional Entities’ performance in providing external review then through an Enforcement Audit process. Second, it is premature to place “Reliability Coordinators” in the Standard. Because NERC has not found that it lacks

Organization	Yes or No	Question 4 Comment (Response page 16)
		sufficient resources to take on the external review responsibility, and thereby has not "designated" any other type of Registered Entity with this responsibility, it is premature for the Standard to make reference to the Reliability Coordinator. See Order No. 706 at P255 ("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). If the Standard Drafting Team is committed to including in its Standard reference to a Registered Entity as having external review oversight, it should wait until NERC makes its designation. Third, assigning external review responsibilities to the Regional Entities (as Reliability Assurers) would facilitate achieving FERC's goal of consistency. Because NERC and the Regional Entities work closely as part of their Regional Entity Delegation Agreement, and because there are fewer Regional Entities than Reliability Coordinators, achieving consistency will be easier if the Reliability Assurers (i.e., Regional Entities) have the external oversight responsibility. Fourth, even if NERC "designates" a Registered Entity (such as, perhaps, a Reliability Coordinator) as having a role in providing external review, the Registered Entity would have the same liability protections as NERC, the Registered Entity is essentially carrying out this role as a NERC-designee. It is easier to capture the roles, responsibilities and liabilities protections through amendment to the Delegation Agreements and Rules of Procedure. In Order No. 706-A, FERC reaffirmed the protections given to external reviewers. See Order No. 706-A at P53 (""we agree [with the ISO/RTO Council] that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself."). These protections include no finding of liability unless intentional misconduct or gross negligence is found. See, e.g., Bylaws at Section 3 (NERC's trustees, officers, employees, and agents are held harmless "for any injury or damage to [any NERC Member] caused by any act or omission of any trustee, officer, employee, agent, or volunteer in the course of performance of his or her duties on behalf of the Corporation, other than for acts of gross negligence, intentional misconduct, or a breach of confidentiality"). Fifth, the combination of R.1.2 and 1.1. and 1.5 in Attachment 1 appears to require an external review by the Reliability Assurer or Reliability Coordinator to exclude assets. This exclusion is contrary to the type of external review identified in Paragraph 325 of Order 706. "However, an external reviewer's role should be limited to determining if additional assets should be added, and should not include making recommendations to remove an asset from the list of critical assets." Clearly the Commission intended to add facilities to the critical assets not exclude them with the external review. does not explicitly describe the nature of the third party review, we interpret the Draft Requirement to not require a Reliability Coordinator/Reliability Assurer to conduct such reviews and/or issue approvals. Clarity could be useful, because others interpret the Standard to require an exception-type external review – i.e., when a Registered Entity does an engineering evaluation that claims that its assets should be classified according to Attachment 1. Others have interpreted the language to require external review of all entities to determine whether they are leaving out assets from

Organization	Yes or No	Question 4 Comment (Response page 16)
		their lists. Sixth, even if the R1.2 is meant only to apply to an external reviewer doing "exception-type" reviews, including this role in the Standards suggests that so long as a Responsible Entity does any type of engineering evaluation, the Responsible Entity can effectively shift responsibility to the external reviewer. Because there is no sanction for incomplete or non-substantive evaluations, the External Reviewers may be deluged with requests to "exempt" assets from the Attachment 1 categorization. This language would effectively undermine FERC's direction that Responsible Entities remain responsible for classifying their assets and they cannot shift this responsible to the Regional Entity or another Organization. See Order No. 706 at P328. In sum, the SRC recognizes that a different set of expectations may apply to those Regional Entities that are also Reliability Coordinators (e.g., WECC). These entities already have liability protections per their NERC delegation agreements, and in their role as Regional Entities, they ultimately have authority over whether the Responsible Entity has correctly identified bulk power system assets as subject to critical infrastructure protection. Similarly, some of the Canadian Reliability Coordinators (e.g., IESO through its enforcement group) exercise similar oversight authority as a Regional Entity with regard to other Registered Entities. While we don't think the nature of this third-party review should be discussed in the standard itself, if the SDT wants to continue to refer to it in the Standard, at this point, the Standard should only refer to Reliability Assurers.
PEPCO	Disagree	If the SDT believes that the big iron approach is the better option, we offer the following comments: Please see below amended Attachment 1. 1. BES subsystem with the following characteristics will be determined to be High Impact (H) unless it has been determined (DELETE not to be essential to the reliability of the BES) that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 1.1. Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2. Each Generation Subsystem whose aggregate output exceeds the value of the Contingency Reserve. 1.3. Each Generation Subsystem that has been pre-designated as Reliability "must run" units. (As identified by the Reliability Coordinator for reliability purposes, not economic dispatch) 1.4. (DELETE Each blackstart Generation Subsystem that has been included in the regional blackstart capability plan.) Cranking Paths and Blackstart Resources that have been included in the System restoration plan that are included in each Generation Subsystem. 1.5. Each Transmission Subsystem that contains (DELETE switching stations substations) operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines (DELETE leaving connected to the station.

Organization	Yes or No	Question 4 Comment (Response page 16)
		1.6. (DELETE Each Transmission Subsystem comprising the Cranking Paths.) 1.7. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) (DELETE or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method) consistent with FAC-10. 1.8. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 1, High Impact Subsystems, including as notified by the Generation Owner. We believe that 1.9 is duplicative with the presence of 1.1-1.4 and 1.8 1.9. (DELETE Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for High Impact Nuclear facilities as determined under Criteria 1.1 through 1.4 above.) We believe that 1.10-1.12 is duplicative with the presence of 1.7 1.10. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse as determined through an engineering evaluation or other assessment method.) 1.11. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. 1.12. (DELETE Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in complete operational failure of the transmission system or separation or Cascading outages.) 1.13. Each Protection System associated with Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an material adverse reliability impact. 1.14. Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.16. Each Control Center and backup Control Center performing Balancing Authority or Transmission Operator functions for transmission assets or generation assets of 2,000 MW or more …… * Each Planning Coordinator and Transmission Planner shall distribute its Planning Assessment results to adjacent Planning Coordinators, adjacent Transmission Planners, and any functional entity that has a reliability related need and that functional entity submits a written request for the information.

Organization	Yes or No	Question 4 Comment (Response page 16)
		If a recipient of the Planning Assessment results provides documented comments on the results, the respective Planning Coordinator or Transmission Planner shall provide a documented response to that recipient within 90 calendar days of receipt of those comments. 2. BES subsystem with the following characteristics will be determined to be Medium Impact (M) unless it has been determined (DELETE not to be essential to the reliability of the BES) that the loss of the subsystem would not result in BES instability, BES voltage collapse, BES separation, or BES cascading sequence of failures through an engineering evaluation or other assessment method approved by the Planning Coordinator and Transmission Planner*, in which case, such Subsystems shall be evaluated to determine whether it has a Medium or low BES Impact. 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 1,000 MVA or more. 2.2. Each Transmission Subsystem that contains (DELETE switching) substations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency stability support. 2.3. Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. 2.4. (DELETE Each Transmission Subsystem identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001-1 for Medium Impact Nuclear facilities as determined under Criterion 2.1 above.) 2.5. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. 2.6. Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above. Regarding 1.1, additional clarity is required. A literal reading of 1.1 could require an entity to update its categorized list of BES Subsystems, if there is any change by any entity anywhere on the grid. This could include changes to the grid brought by natural disasters such as ice storms or hurricanes. Consider: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the Responsible Entity commissioning new BES Subsystem(s), decommissioning BES Subsystem(s) or being notified by a transmission planning authority of changes in the electric system that could affect the impact of the Responsible Entity's BES

Organization	Yes or No	Question 4 Comment (Response page 16)
		Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. Regarding 1.2, the industry would be aided by the provision of examples of approved engineering evaluation methods. We believe that the standard should either better define an acceptable/minimum engineering evaluation that needs to be performed or specify the ability of individual entities to determine they are allowed to determine the engineering evaluation that they will perform. If the standard is going to specify external review they need to provide some guidance on what the level of review is going to be and the items that need to be considered for the review. We are concerned about the designation of Reliability Assurer as being responsible for this oversight role. The Reliability Assurer may not have sufficient resources or expertise to satisfy the obligation. It may be more appropriate for the Planning Coordinator and Transmission Planner to perform this task, subject to review.
NEI	Disagree	A) Beginning the process using R1 & Attachment I is illogical for addressing this cyber security puzzle, and only obfuscates the issues truly salient to the solution set. B) R1/Attachment I create a great deal of unnecessary ongoing work and regulatory exposure. C) Clear delineation of exactly what constitutes a “BES Subsystem” in practice in any number of various scenarios is elusive at best. D) Is it appropriate to require Reliability Coordinators to accept responsibility for ‘approving’ and/or ‘validating’ “engineering or other assessment methods?” If the Reliability Coordinator is found to have been mistaken after the fact, who will be accountable? What if the mistake involves Entities whose operation spans more than the aegis of an individual Reliability Coordinator? Frequently from a generator owner/operator perspective they don’t know the impacts without contacting the Transmission Owner. Where either the Reliability Coordinator/Reliability Assurer is used for the evaluation, who reviews? Do we have a need for an Independent Third Party Review? In this case, the Reliability Coordinator/Reliability Assurer needs to provide acceptable evaluation methodology E) In practical terms, 30 days is a very narrow time window for what’s required. F) Is the expectation that the engineering evaluation is in place at T=0, is there an exclusion timeframe to enable the evaluation to be performed and approved? G) Item 1.1: The team should consider a separate requirement for this such that a Lower VRF can be applied. Merely updating a list within 30 days is a documentation item that should not be subject to a High VRF penalty. H) Item 1.2: NEI believes that the need for RC or RA approval can be avoided by requiring the study follow the PC’s Methodology for identifying IROL as defined in FAC-010/FAC-014. Furthermore, we do not support the use of the RA. The RA is a Functional Model Guideline (which we did not support) and the NERC registration criteria for responsible entities do not support the RA classification. I) I) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to

Organization	Yes or No	Question 4 Comment (Response page 16)
		a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low."

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies)

2.2 The Responsible Entity name

2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: The SDT thanks all respondents who commented on this requirement. In consideration of the overall comments received, the more direct statement of the impact categorization of BES Cyber System makes the requirement for notification unnecessary. This requirement no longer exists in the revised draft of CIP-002-4 (now CIP-010-1).

Organization	Yes or No	Question 5 Comment (Response page 17)
Progress Energy	Disagree	Add a new bullet "2.4 Basis for categorization change." NERC needs to better define or explain "directly interconnected". NERC needs to have CIP-003 through -009 Version 4 defined before we can commit to "within 30 calendar days of developing or updating its BES impact categorization."
Dynegy	Agree	
GSOC/OPC	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2. We suggest changing "Transmission Subsystem owners" to "Transmission Subsystem owners and operators."
Hayden	Agree	I would also suggest that the information also include a) method of notification, b) date of notification
SDGE	Disagree	Transmission Subsystem owners must have input on categorizing the impact that a Generation Subsystem will have on the transmission system; in many cases, the Generation Owners / Operators don't have access to the appropriate

Organization	Yes or No	Question 5 Comment (Response page 17)
		engineering data to make such a determination. With all of the effort required to gather this data and analyze it thoroughly, 30 days may not be enough time. This time period includes the time required to gather data, perform studies and then get approval from the Reliability Coordinator. We propose a 30 day timeframe for providing the results and analysis to the RC. What is the definition of "accurate information"? Need clarification on ownership of generation subsystems; does this mean that this Requirement is not applicable for non-company owned generation subsystems? Need guidance on compliance for company-owned generation subsystems that are operated by other entities. Finally, this requirement could force the exchange of confidential information between entities. Standards CIP-003-4 and/or CIP-004-4 should take this into account when they are revised.
APPA	Disagree	We disagree with the need for BES Subsystem identification as discussed below under Question #6.
Consumers	Disagree	Changing classification will, in most cases, result because the transmission operator or reliability coordinator changed something. As such, this isn't likely to occur without the transmission operator or reliability coordinator knowing it first. This requirement needs to be for the Transmission Subsystem owner to notify the generator operator and generation owner when conditions change such as to make a generation subsystem potentially change categories. This identifies only one way communications from the generation provider to the transmission provider. It should be in both directions. In addition, Transmission Owners/Operators/Providers and Load-Serving Entities need to be exchanging information in a similar fashion. In addition, the current required shared information is not adequate. The critical function that the asset is providing needs to be shared. Also, at least the cyber system needs to be identified, but possibly details about such may also need to be shared.
NPCC	Agree	
MPPA	Disagree	MPPA supports the requirement to report the identification of High and Medium impact generation subsystems. However, as written, this requirement does not place the same burden on Transmission Owners to report their High and Medium impact systems.
Central Lincoln	Disagree	See answer to #4.
NERC	Agree	1. Ensure the language captures notification of all transmission elements in a Cranking Path for any identified blackstart generation resources. 2. In order to support compliance activities, add the following and update the Measures section appropriately: R2: add text to require the documentation identified to be signed and dated (by proper personnel identified per CIP-003 / R2). 3. Requirement R2 – change "developing" to "determining" in line 6.

Organization	Yes or No	Question 5 Comment (Response page 17)
Dominion	Disagree	Although Dominion agrees with most portions of R2, Dominion suggests the following modifications: "…..shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide written notification to the Primary Compliance Contact of the Transmission Owner or Distribution Provider to which the BES generation asset is directly interconnected …." A Responsible Entity that owns any Generation Subsystem is prohibited, in many cases, from access to the data necessary to determine whether its facility could affect or influence the impact of BES Subsystems on the Bulk Electric System. Dominion believes, therefore, that in many cases, the Reliability Assurer, Transmission Planner or Resource Planner must make this determination and notify the Generator Owner of the results of their impact determination (e.g., high or low).
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	The purpose states that the Generators Owners categorization would not be proper unless the Transmission Owner has the Generator Owner's security control information. This requirement is unnecessary and should be deleted as it is covered between R1 and R3.
Dyonyx	Agree	
MISO	Agree	
Westar	agree	
Green Country	Disagree	Why not change it from a bottom up approach to a TOP down request approach for the initial categorization. i.e. Transmission Operator requesting from GO/GOP. Then upon registered entity updating a system use a bottom up outlined here. It would make the flow of data and control of it a lot smoother.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE	Disagree	The first two clauses of the Requirement, "To support . . ." and "to ensure . . .," are purpose statements that don't seem to be appropriate to include in a requirement. Do these clauses include an obligation for TOs to classify their equipment that interfaces with a Generation Subsystem in the same way that the Generator Owner does? If so, this could cause a "race to the top" in which equipment rated by one Responsible Entity rates at a Medium BES Impact and rated by another Responsible Entity rates at a High BES Impact would have to be rated High by both entities. This would render the categories less meaningful.

Organization	Yes or No	Question 5 Comment (Response page 17)
PSEG	Disagree	Comment #1: This requirement seems to duplicate our understanding of the goal of Requirement 1 and therefore should be deleted. In order for an entity to meet the intent of Requirement 1 they need to understand both the BES Cyber System being reviewed and the elements that could be compromised through that BES Cyber System. In other words if a BES Cyber System can influence both a Transmission Substation device and a Generating Plant's device then both have to be considered as a single subsystem and identified as such for requirement 1. Example: A BES Cyber System if compromised allows access to both elements in a transmission substation and a generating plants production has to be identified per requirement 1 as a single subsystem. In addition to our concern that this standard is duplicative to requirement 1 we have a concern with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Example: Standards CIP-003 through 009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control. One specific concern is if someone was terminated with cause an entity has a limited amount of time to remove that person's access. Because this requirement is requiring the sharing of information an entity may not be able to secure the necessary commitments from different parties that termination information (this example) is communicated within X amount of time. Comment #2: This is an improvement on the current approach, however we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is High, should they notify the generation subsystem owner? For all future assessments as well? Further we are concerned in regards to a subsystem being classified differently and approved as such by two different RC's. Comment #3: Changing classification will, in most cases, result because the transmission operator or reliability coordinator changed something. As such, this isn't likely to occur without the transmission operator or reliability coordinator knowing it first. This requirement needs to be for the Transmission Subsystem owner to notify the generator operator and generation owner when conditions change such as to make a generation subsystem potentially change categories.
WE-Energies	Disagree	While Wisconsin Electric Power Company feels this approach of reviewing defined asset impact categorizations with connected transmission operators, the current requirement does not address areas around handling discrepancies of categorization between Transmission Operator and Generator Owner/Operator.

Organization	Yes or No	Question 5 Comment (Response page 17)
Idaho Power	Agree	
SOCO	Disagree	In the High and Medium categories, generation subsystems are allowed 30 days to submit information to the Transmission subsystem owners. We suggest that this same 30 day grace period be allowed in the Low category as well. Suggest that 2.1 be revised to read “and other identifiers which may assist in identifying the Facility(ies)”
DTE	Agree	
AEP	Disagree	Refer to question #2 above.
Edison Mission	Agree	
Calpine	Disagree	A regional authority would be the better responsible entity for this requirement.
NS&T	Agree	We agree with this proposal in principle, but we note that the proposed requirement does not specify what Transmission asset owners/operators must (or must not) do with the information they have been given. Would the Transmission asset owner/operator be compelled to change their subsystem categorization if the Generation asset owner/operator had designated their subsystems at a higher impact level? If so, could the Transmission asset owner/operator challenge this forced upgrade? Who would adjudicate such a challenge? We also wonder if this proposed requirement could create difficult non-disclosure issues in some cases. At the very least, the information that Generation asset owners/operators are directed to share would be considered "protected information" under the *current* Standards.
Flathead	Agree	This seems reasonable for High or Medium Impact facilities, but prefer annual requirements to lessen the paperwork burden.
E ON	Disagree	The requirement implies a Transmission Subsystem owner’s input into the categorization of unaffiliated Generation Subsystems. R1 already provides a Reliability Coordinator backstop role in reviewing and insuring proper categorization of BES Subsystems. E ON U.S. is also troubled by the statement: “. . . to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets.” The Transmission Subsystem owner alone should be responsible for identifying security controls for all owned transmission assets.
Carthage		CWEP has no comments for 5.
WECC	Agree	
Entergy	Disagree	This is an exercise in meaningless administration and inter-organizational coordination, with tangible unsavory regulatory consequences for failure which provide no practical benefit to anyone, much less reliability of the BES.

Organization	Yes or No	Question 5 Comment (Response page 17)
LCRA	Agree	
FRCC		In the main body of the requirement it states that the Generation Subsystem owner has to provide certain information to the Transmission Subsystem owners that are directly interconnected to them. This may seem to be a nit, but how will a Generation Subsystem owner know who has Transmission Subsystems? The compliance registry or functional model does not have a function for that and there are only TO's and TOP's registered. If the definitions are removed after consideration of previous comments, it may be something for the drafting team to think about in terms of other registered functions. In addition, the information that is required to be shared can be extremely confidential and there is no requirement for how this information will be maintained by those that receive it.
NIPSCO	Disagree	We believe this is an improvement on the current approach; however we are concerned with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Additionally, we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is high, should they notify the generation subsystem owner? Further we are concerned in regards to a subsystem being classified differently and approved as such by two different RA's / RC's. Suggestion: Clarify the responsibility of all entity types for information sharing and clarify the intended information protection requirements.
ConEd	Disagree	The Standard should stipulate an implementation requirement: the GO's categorization must be shared with the Regional Entity within 6 months of the Standard approval by FERC. The RE must in turn must share (within 30 days) the categorization with any impacted TO's.
O&R	Disagree	The Standard should stipulate an implementation requirement: the GO's categorization must be shared with the Regional Entity within 6 months of the Standard approval by FERC. The RE must in turn must share (within 30 days) the categorization with any impacted TO's.
Alliant	Agree	We believe the introductory statement : To support the . . . security controls for their assets," adds nothing to the requirement and should be deleted.
Ameren	Agree	
Black Hills	Agree	What happens in a jointly owned situation where the TOP receives two different assessments of impact? Which prevails?
TNMP	Disagree	TNMP supports the approach of requiring those with access to information to be responsible for providing it to other Entities that need the information. However, the 30 calendar day notice is not enough time to make a Transmission Subsystem CIP-compliant if its impact rating were upgraded (e.g. Low to Medium or Medium to High). If the Generation Subsystem change is planned, then the notification needs to be a point far earlier than 30 days from when the actual change occurs. Twelve calendar months should be standard to guarantee that CIP-compliance projects, which can incur significant costs, can be incorporated into annual fiscal budgets. An alternative would be for the Responsible Entity of the

Organization	Yes or No	Question 5 Comment (Response page 17)
		impacted Transmission Subsystem to have 12 calendar month once notified of a change to bring the Transmission Subsystem into compliance, as is provided for unplanned changes
NVEnergy	Disagree	We disagree for two reasons: First, the team should observe strong caution about the communication of Impact Categorization data. In the current version of CIP-003, there are strong controls specified around the protection of information related to Critical Assets and Critical Cyber Assets. In fact, even the lists of such Assets are themselves to be protected and cannot be revealed to individuals without a proper clearance via Personnel Risk Assessment and requisite Cyber Security Training. This Requirement as proposed seems to open a door to release of sensitive information worthy of high security protection to virtually unknown and un-verified parties, and would be a clear violation of the existing requirements related to Information Protection programs as specified in the existing CIP-003. Second, the 30-day period is overly burdensome on the industry. As well, it is not understood how a Transmission subsystem owner could be unaware of the characteristics of an interconnecting generation subsystem, which would necessitate such notification. As stated previously, the focus should be upon those cyber systems that can have measurable impact upon the reliability of the BES.
Empire	Disagree	I disagree with the 30 day requirement and would suggest that the 30 days be moved to allow 120 days. This will allow entities who require higher authority approvals enough time for proper notification.
SWTC	Disagree	Subsystems add an Unneeded Step and Adds Confusion: • Several have pointed out that we can get to the same classification analysis by either defining subsystems and then determining their impact on the BES, or starting directly with the worst case scenario analysis of a malicious use of a cyber system. Hence, some of us have questioned the purpose of adding the step of defining Subsystems to the analytical process, which seems unneeded. • In addition, since the draft does not define how groups of Facilities are to be grouped into cybersystems, than how do we know if the groupings themselves are correct and auditable. I can envision a situation where the auditors disagree with the entity on how Facilities are to be grouped into subsystems. Or would we get into the same situation where entities are allowed to define subsystems however they want and a potential for mistrust by regulators that we may have manipulated the definition of these subsystems in a way that causes us to avoid much of the CIP standards? • It may be simpler, more straightforward and less confusing to skip the step of defining subsystems and simply ask ourselves the question: What's the worst case scenario that can be caused by a malicious use of a cyber system? • This will cause us to have to inventory all of our cyber systems, but, I don't believe we were ever going to avoid that, even with defining subsystems.
SCEG	Agree	
Exelon	Disagree	In order to avoid possible confusion with Organizational registration we suggest that the SDT replace the “Transmission

Organization	Yes or No	Question 5 Comment (Response page 17)
		Subsystem owners", with "owner of the Transmission Subsystem". In addition we believe that the current wording in the CIP Information Protection requirements will need to be revised to allow for the sharing of information as stated in this requirement.
BPA Trans	Disagree	Recommended Changes With the addition of new requirement #1, existing R2 becomes R3. We believe that this requirement is too narrow in scope, that it should also be applicable to other Subsystem owners. We have edited the requirement based on this belief: Requirement 3 R3. The Responsible Entity that owns any BES Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Subsystem, provide the following information to those Subsystem owners directly interconnected to that Subsystem: (Violation Risk Factor: High) R3.1. Description of the Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies) R3.2. The Responsible Entity name R3.3. The BES impact categorization level Observation- There are potential situations where this type of communications requirement should also apply to Transmission and Control Center Owners, it is not just a Generation issue.
HQT	Agree	
Allegheny Energy	Disagree	Although this is an improvement on the current approach, we are not sure how the situation may be resolved where a GO categorizes a generation subsystem as "High" but the directly connected transmission subsystem owner does not categorize the generation subsystem as High. Also, if the converse were to happen, it is not clear if the transmission subsystem owner needs to notify the generation subsystem owner? Furthermore, we are concerned in regards to a subsystem being classified differently and approved as such by two different RC's.
KCPL	Disagree	Requirement 2.3 implies the Registered Entity to establish an impact categorization level. It some cases it will not be possible for Generator Owners to know the impact their generator has even with appropriate criteria. Consider the example of an IPP with one 500 MW generator surrounded by a robust Balancing Area of transmission facilities and generating facilities. This may be a LOW or NO IMPACT reliability impact. Consider the same IPP in an isolated area starved for reactive voltage support. This could be a HIGH. The Transmission Operator or the Reliability Coordinator would be the appropriate entity to apply appropriate criteria and establish an impact level. The Standard needs some additional thought as to the process to consider when multiple facilities are brought together and the requirements to establish an appropriate categorization level.
Connectiv Energy	Agree	

Organization	Yes or No	Question 5 Comment (Response page 17)
MidAmerican	Disagree	Modify CIP-002-4 R2 to maintain the list of BES assets (instead of Critical Assets). BES bright line criteria also eliminate the need for proposed CIP-002-4 R2 that addresses directly interconnected facilities. All facilities are held to the same bar across the industry.
CPG	Disagree	GO/GOPs lean heavily on TO/TOPs in assessing their assets as the TO and the TOP have a wider system view of the BES than the GO/GOPs do. For example, a large generating facility may not be as critical to the BES as a smaller facility in a critical area. This Requirement should be reworded to ensure that the TO/TOP and GO/GOPs have an open dialogue as to how they categorize their assets and how they affect the assets directly connected to them.
Santee Cooper	Disagree	See comment for #4.
OGE	Disagree	The Transmission Subsystem Owner is dependent on the quality and timing of the Generation Subsystem Owner. There is risk that the Transmission Subsystem Owner and Generation Subsystem Owner may have differences in the impact categorization.
Oncor	Agree	We feel the introduction statement “To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets,” adds nothing to the requirement and could be deleted.
PPL Supply	Disagree	Agree with the need for Generation Owners to notify TOs of changes, but also there exists a need for reciprocal communication of Generation asset inclusion in system restoration plans or reliability must run status, and results from system reliability or stability analyses for which Generation asset owners have no data to perform independent analyses yet determine the asset’s impact on the reliability of the BES.
St. George	Agree	
NGRID	Disagree	Please clarify 2.2 – which Responsible Entity – GO or TO? Another concern is that Standards CIP-003 through CIP-009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control.
MGE	Disagree	This information is already provided within the following NERC Standards: FAC-001-0, FAC-002-0, FAC-009-1, PRC-001-1, PRC-015-0, TOP-005-1.1. Please clarify why the owner of the Generation Subsystem is required to notify the Transmission Subsystem owners directly interconnected to that Generation Subsystem and what the Transmission Substation owner is to do with the information once it receives it? This will also place an undue burden on the Transmission Subsystem owner when they initially determine that one of their subsystems may be Low BES Impact but the Generator Subsystem owner determine that their subsystem is Medium or High BES Impact. This will cause the Transmission Subsystem owner to elevate the impact of their facility to

Organization	Yes or No	Question 5 Comment (Response page 17)
		equal the Generator Subsystem category. Many companies are not vertically integrated and this cause serious non compliance issues. In order for R2 to have the maximum positive impact on assuring an adequate level of reliability, the Transmission Subsystem owner would also need to inform the Generator Subsystem owner the same information when a Transmission Subsystem is categorized as a High BES or Medium BES Impact for those Subsystems that are connected to each other.
FE	Disagree	R2 correctly requires a Transmission Subsystem owner to consider connected generation but improperly confines the consideration to Generation Subsystems. The problem with R2 is that it does not allow for the possibility that a substation which is part of a Transmission Subsystem may be serving a set of generators, that while not a Generation Subsystem in and of itself, is > 2000 MW or meets another BES Impact threshold. In such a case, the Transmission Subsystem should adopt a BES Impact that is a function of the generation characteristic as well as the transmission characteristic, i.e., the higher of them. In other words, the Transmission Subsystem owner must consider connected generation as a general matter, outside of the generators' potential Cyber System. Consequently, the Transmission Subsystem owner requires no notification by the generator – the Transmission Owner will already have general information about its connected generation. Therefore, R2 is not needed, and Attachment 1 should be modified to expand the scope of Transmission Subsystem thresholds to consider the size and scale of its connected generation. For example, Attachment 1 1.1 should require a High BES Impact for "Each Generation Subsystem or Transmission Subsystem exclusively connected to generation with aggregate rated name-plate generation of 2,000 MVA..."]
TECO	Agree	We believe that there should be direction within the standards as to how the Transmission Subsystem Owner should categorize its subsystems based upon the categorization of the generation subsystem.
CECD	Disagree	1. The phrase "to support the proper categorization of BES subsystems as identified in R1" should be deleted because the Purpose of the standard has already been stated. 2. If High and Medium category BES subsystem information is going to shared, notification requirements applying to parties of High or Medium status should apply to all Responsible Entities and not be limited to communication by a Generation Subsystem to a Transmission Subsystem owner.
MRO	Agree	We feel the introduction statement “To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets,” adds nothing to the requirement and should be deleted.
GTC	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2.

Organization	Yes or No	Question 5 Comment (Response page 17)
		We suggest changing “Transmission Subsystem owners” to “Transmission Subsystem owners and operators.”
Xcel	Agree	
BGE	Agree	We support this notification proposal and approach as it encourages information sharing between generation and transmission owners. It would be beneficial to also add Transmission Operators as a party of this Requirement.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Consider removing this requirement. It is not clear why a Transmission Subsystem owner would need to have information on the ranking of Generators. In cases where the Generator is an independent entity from the Transmission Owner, revealing some of these information may result in a question of confidentiality. Generator Owners for the Generator Subsystem are generally not able to adequately perform an assessment of the impact of their Transmission Subsystem; the Transmission Providers themselves would be able to make this assessment much better as they have real-time operating data to perform such an analysis.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes this is an improvement over the current approach, however we are concerned as to how a situation may be resolved if a Generator owner determines a subsystem is High and the directly connected transmission subsystem owner does not determine the generation subsystem as High. Likewise, the language does not seem to flow in the opposite direction; if the transmission owner believes a generation subsystem is High, should they notify the generation subsystem owner?
FMPA	Disagree	Again, Subsystem is an unnecessary and redundant step in the process. FMPA does not see a reliability need for this requirement and we recommend removing it. Transmission Owners / Operators and Generation Owner / Operators will be using the same criteria of Attachment 1, so, in what scenario will they arrive at a different answer for the same Subsystem?
Duke	Disagree	We disagree with the approach of categorizing BES Subsystems, but do agree that communication and coordination is required when entities make changes to Cyber Systems and security controls that could impact interconnected entities.
NBSO	Agree	
AESI	Agree	We agree, but add the following comments: It may be equally important for the transmission subsystem owners to provide relevant information to the generation owner(s) such that studies such as those described in Attachment 1, bullets 1.1 and 2.1 can be carried out by the generation owners or to provide the generation owners with the results of such studies which have been carried out by the transmission owner and approved by the reliability coordinator, etc. in order to allow the generation owners to comply with R1 and R1.2. We suggest changing “Transmission Subsystem owners” to “Transmission Subsystem owners and operators.”

Organization	Yes or No	Question 5 Comment (Response page 17)
IESO	Agree	
Manitoba 2	Agree	
OMPA	Disagree	OMPA agrees with the communication requirements; however, does not agree with the requirement to identify the BES subsystems.
ATC	Disagree	This requirement seems to duplicate our understanding of the goal of Requirement 1 and therefore should be deleted. In order for an entity to meet the intent of Requirement 1 they need to understand both the BES Cyber System being reviewed and the elements that could be compromised through that BES Cyber System. In other words if a BES Cyber System can influence both a Transmission Substation device and a Generating Plant's device then both have to be considered as a single subsystem and identified as such for requirement 1. Example: A BES Cyber System if compromised allows access to both elements in a transmission substation and a generating plants production has to be identified per requirement 1 as a single subsystem. In addition to our concern that this standard is duplicative to requirement 1 we have a concern with entities being required to share sensitive BES information with no clear additional obligations associated with CIP-003 – 009. Example: Standards CIP-003 through 009 contain several requirements about training and access to critical asset information. By requiring the sharing of critical information entities could be exposed to non-compliance violations for situations they have little or no control. One specific concern is if someone was terminated with cause an entity has a limited amount of time to remove that person's access. Because this requirement is requiring the sharing of information an entity may not be able to secure the necessary commitments from different parties that termination information (this example) is communicated within X amount of time.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 5 Comment (Response page 17)</th></tr>
<tr><td></td><td></td><td>appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Agree</td><td>Puget Sound Energy agrees with the notification process. The aspect of a GO that is independent of the BA/TOP performing their own categorization still leaves the opportunity for inconsistent categorization across a system meaning all the Transmission Subsystem could be determined to be High and all the supporting Generation Subsystems to be Low. If the intention is to ensure reliability operation there needs to be a method of gaining consistency.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA has concerns about the privacy and confidentiality of this important information to other entities and how this information will be kept or who will have access to it. This process needs to ensure that confidentiality agreements are in</td></tr>
</table>

Organization	Yes or No	Question 5 Comment (Response page 17)
		place with the recipients. If this information needs to be provided to the Transmission Subsystem owners, what entity will be responsible to ensure the entities who need to provide this information receive a listing of the appropriate Transmission Subsystem owner(s)? IMPA recommends that Generation Subsystem owners provide their information to the Reliability Coordinator who will be responsible for providing it to the appropriate Transmission Subsystem owner(s).
ERCOT	Disagree	ERCOT ISO recommends that the requirement be revised to make the required action more prominent in the wording of the requirement. Justification information is not necessary. "Each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem."
PacifiCorp	Disagree	Modify CIP-002-4 R2 to maintain the list of BES assets (instead of Critical Assets). BES bright line criteria would also eliminate the need for proposed CIP-002-4 R2 that addresses directly interconnected facilities.
NEI	Disagree	A) To avoid confusion with organizational registration, replace "Transmission Subsystem Owners" with "Owners of the Transmission Subsystem". B) R2 rightly requires a Transmission Subsystem owner to consider connected generation but improperly confines the consideration to Generation Subsystems. The problem with R2 is that it does not allow for the possibility that a substation which is part of a Transmission Subsystem may be serving a set of generators, that while not a Generation Subsystem in and of itself, exceeds 2000 MW or meets another BES Impact threshold. In such a case, the Transmission Subsystem should adopt a BES Impact that is a function of the generation characteristic as well as the transmission characteristic, i.e., the higher of them. In other words, the Transmission Subsystem owner must consider connected generation as a general matter, outside of the generators' potential Cyber System. Consequently, the Transmission Subsystem owner requires no notification by the generator – the Transmission Owner will already have general information about its connected generation. Therefore, R2 is not needed, and Attachment 1 should be modified to expand the scope of Transmission Subsystem thresholds to consider the size and scale of its connected generation. For example, Attachment 1 1.1 should require a High BES Impact for "Each Generation Subsystem <u>or Transmission Subsystem exclusively connected to generation</u> with aggregate rated name-plate generation of 2,000 MVA …"] C) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High

Organization	Yes or No	Question 5 Comment (Response page 17)
		results in “Medium”; and that Medium-Low and Low-Medium results in a “Low.”

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: Respondents commented that attachment 2 (Reliability Functions) was overly broad and open-ended, and that the focus should be on real-time systems. Many commented on the potential absence of correlation between the impact level of the BES Subsystem and the impact of the associated BES Cyber Systems on the functions. Others commented that the categorization methodology should be similar to that described in the concept paper. Some noted that risk should be considered, not just impact: many cited connectivity as a factor. Some commented that there should be a "No Impact" category.

In consideration of these comments, the SDT has made substantial changes to the requirements. The categorization requirement is no longer based on an inherited categorization based on the impact level of the BES Subsystem, but each BES Cyber System is categorized based on its impact on BES Facilities which perform reliability functions. The scope has been clarified: BES Cyber Systems in scope are those which impact real-time operations of the BES.

Organization	Yes or No	Question 6 Comment (Response page 18)
Progress Energy	Disagree	We believe Attachment 2 goes beyond what should be the scope of the CIP standards and the focus needs to be on real-time cyber operations. In addition, CIP-003 through -009 Version 4 needs to be defined before we can agree to this requirement.
Dynegy	Agree	
GSOC/OPC	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with the BES Cyber System itself.

Organization	Yes or No	Question 6 Comment (Response page 18)
		We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will far outweigh its benefits. It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
Hayden	Agree	
SDGE	Agree	
APPA	Disagree	APPA Task Force Comments: CIP-002 – Attachment 2: Functions Critical to the Reliable Operation of the Bulk Electric System The APPA Task Force recommends that the SDT either eliminate Attachment 2 or convert it to a reference/guidance document supporting the standard. The important criteria of the standard are included in Attachment 1. The conceptual discussion of functions in Attachment 2 only adds redundancy, complexity and confusion. If Attachment 2 identifies "functions critical to the reliable operation of the Bulk Electric System," there should be a one-to-one mapping of these functions to each of NERC's other reliability standards. Also, how are these functions different from those described in the Functional Model? Is Attachment 2 essentially another, different, functional model? At best, Attachment 2 should be treated as a list of "things to consider" when developing worst case scenarios/contingencies for evaluating the impacts of "unavailability, degradation or compromise" of a Cyber System. If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? Unless Attachment 2 is treated as a guidance document, the identification of reliability functions cannot be open-ended, implying that additional functions, or aspects of functions, have yet to be identified. The SDT should avoid open-ended statements such as: "Aspects of the Managing of Constraints include, but are not limited to" that are followed by a bulleted list. Further, the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. From this perspective, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is certainly NOT critical. Calculation of ACE is certainly NOT critical since ACE values are double-checked with neighboring BAs on separate Cyber Systems, ensuring identification and correction of errors. This standard should focus on what is truly critical: threats of an Adverse Reliability Impact resulting in "instability, uncontrolled separation, or cascading" outage. If Attachment 2 is retained, APPA suggests that it should be renamed: "Activities Performed to Maintain the Reliable Operation of the Bulk Electric System."
Consumers	Disagree	This needs to be based on the cyber systems that are at risk. The definition of BES Cyber System is not appropriate. If "BES Cyber System" is replaced with "critical cyber assets", then this would be appropriate. But that would lead us back

Organization	Yes or No	Question 6 Comment (Response page 18)
		to where we are now, so there is no need to change the existing standard. As we have noted earlier, this "inheriting" of the same BES impact from the subsystem is flawed. In such a scenario, a printer would inherit the same category as a server. This is the same issue that was identified as a problem in the earlier versions of CIP-002 that the SDT seemed to be trying to move away from. Each RE should categorize and list those cyber assets associated with a High Impact subsystem (as recommended, medium and low terminology not used) but not list those with no impact. For those listed, a second evaluation of the cyber assets should then be performed and recorded, eventually in the cyber asset list.
NPCC	Agree	
MPPA	Agree	
Central Lincoln	Agree	Central Lincoln agrees with this in general, but please consider the APPA Task Force comments regarding attachment 2.
NERC	Agree	1. In order to support compliance activities, add the following and update the Measures section appropriately: R3: add text to require that the documentation created when categorizing and subsequent documentation called for in R3.1 & R3.2 to be signed and dated (by proper personnel identified per CIP-003 / R2). 2. Requirement R3.2 – add the word "level following "same BES impact" in the first sentence.
Dominion	Disagree	The function performed by the cyber system as well as the criticality of the BES Subsystem should be examined to identify the criticality of a BES Cyber System.
Encari	Disagree	As earlier commented we feel that Attachment 2 can be strengthened to include additional components - the actual requirements above we do agree with.
US ACE – NW	Agree	
SCE	Disagree	A cyber system supporting a BES subsystem may not always warrant the same impact level as suggested by Requirement 3.2. Factors such as: (a) the role of the BES cyber system within the broader context of the operation of the BES subsystem (Is this the only mode of failure of the BES subsystem?); (b) the technical capabilities of the cyber system (Does it provide information sensing capability or interactive control?): (c) the nature of the network that the interconnected BES cyber system is using (IP or serial); and (d) the connectivity if any outside a BES sub-system (Is remote access allowed?); are examples of the factors to consider. Impact level determination can be a combination of the function (as listed in Attachment 2), the impact level of the BES subsystem, and the degree to which it is interconnected. The interconnectedness of a cyber system is a significant contributor to its security vulnerabilities.
USBR	Disagree	It is sufficient that the BES systems are assessed to have an impact. The degree of an impact is superfluous.
Dyonyx	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
MISO	Agree	
Westar	Agree	agree with the concept of the highest impact level being assigned. I do think that Attachment 2 just adds confusion and should be eliminated.
Green Country	Agree	
Oregon PUC		No comment
NB Power Gen	Disagree	3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that [is connected bi-directionally (routable protocol, modem) outside of the perimeter of the electronic security perimeter contained within the facility it is installed in and, if accessible remotely] has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.
Manitoba 1	Agree	
Portland GE	Disagree	Requirement 3.2 could spur a “race to the top” in which everything connected to a High BES Impact system would have to be rated High as well. This could provide incentives to Responsible Entities to keep their systems disconnected because connecting them would bring them all under the scope of a higher level of controls. For example, Section 3.2 uses the term “associated.” However, everything could be interpreted as “associated” and may “affect” the Subsystem. The SDT should recognize that even though a Cyber System may affect or be associated with a BES Subsystem, it could have little impact on the BES, regardless of the Subsystem’s impact on the BES.
PSEG	Disagree	Comment #1: We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problem from CIP Version 1). Comment #2: We believe that this needs to be based on the cyber systems that are at risk. The definition of BES Cyber System is not appropriate. If “BES Cyber System” is replaced with “critical cyber assets”, then this would be appropriate. But that would lead us back to where we are now, so there is no need to change the existing standard. Suggestion: 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber

Organization	Yes or No	Question 6 Comment (Response page 18)
		System associated with its Transmission Subsystem, Generation Subsystem or Control Center.
WE-Energies	Disagree	Wisconsin Electric Power Company contributed to and supports EEI's comments regarding this question. In addition, Wisconsin Electric Power Company feels there is potential for confusion in R3.1, because some systems touch so many other BES "subsystems".
Idaho Power	Disagree	Cyber systems may have varying levels of impact on the functionality of the BES Subsystem and therefore, may not need the same level of protection. To categorize every cyber system at the same level as the BES subsystem adds an unnecessary burden on the registered entities.
SOCO	Disagree	This is a bit troubling that all the pieces have to take on the criticality of the highest impact level of the parts. The listing of the Cyber System should be based on a top down approach rather than a bottom up approach. Only after a BES Subsystem is classified as a High or Medium Impact, should the Cyber System related to it should be classified as High, Medium Impact. This will provide a more functional approach that will provide the same result while being less resource intensive. The control system for a Generation Unit may be classified as a High Impact, but classification of a pH monitor or ambient air sensor connected to the control system, not essential for generation operation should not required to be classification at the High classification. Suggest wording – Each Responsible Entity shall list each BES Cyber System which is critical to the operation of the BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any Functions Critical to the Reliable Operation of the Bulk Electric System. Delete entire paragraph - "For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."
DTE	Agree	
AEP	Disagree	Refer to question #2 above. The SDT took a good start in Appendix 2 of segmenting the standard into a functional approach. However, we believe that this section is not yet fully developed and should be comprehensively reviewed by SMEs to determine and describe, on a bright line basis, what is specifically in scope and out of scope for each of the functional areas. While helpful in better defining the functional areas, the use of the exhaustive list of descriptions leads to interpretation issues of what is meant to be included and not included by the descriptions, and will not get to the bright lines that are sought to define what specifically needs to addressed.
Edison Mission	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	As I read this multiple medium impacts equal a high, does not make sense. Either it has one high or not.
E ON	Disagree	E ON U.S. does not agree with assigning each cyber system the same level of criticality as the most impactful subsystem. Some cyber systems associated with a generating station, for example, do not impact the BES if disabled (e.g., emissions monitoring systems).
Carthage	Agree	
WECC	Agree	
Entergy	Disagree	The size/rating of a "BES Subsystem" (whatever that is – say, for sake of discussion, a substation) has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. A 69kV substation with a routable network link to its control host data center presents much higher adverse cyber security risk than an EHV substation served only by legacy serial communication lines to its control host. Pick any "BES Subsystem" and this fact remains the same.
CenterPoint	Disagree	Disagree – See comments to 1.a. It is unclear what the SDT hopes to accomplish with this requirement when compared to the existing requirements under CIP-002, especially when this proposal has been unveiled in a piecemeal fashion. If the SDT's intent is to extend a set of cyber security requirements to non-critical cyber assets, the SDT could propose such a set without the contortions and flaws of this proposed new classification system. Moreover, it may not be appropriate for a BES Cyber System to automatically inherit the impact of the associated BES Subsystem because the cyber system may not be essential to the operation of the associated BES system, a concept correctly captured by the existing CIP-002 standard. Furthermore, if the SDT were to leave the definition of cyber systems as proposed in this draft, cyber security risk would also have to be considered in determining the impact level of the cyber system. For example, a Cyber System that does not use a routable or dial-up connection to communicate externally should be categorized as low impact because it is not vulnerable to remote attacks, regardless of the impact of its associated BES Subsystem.
LCRA	Agree	
NIPSCO	Disagree	We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problems from CIP Version 1). Suggestion: Eliminate the BES protection level inheritance. Allow the cyber assets to be evaluated based on the impact to the asset, not based on the impact of the asset to the BES. If this inheritance approach is left as proposed by the SDT,

Organization	Yes or No	Question 6 Comment (Response page 18)
		we would need to see how the one size fits all approach is being addressed throughout CIP-003-4 through CIP-009-4.
ConEd	Agree	
EEI	Disagree	EEI believes that it is appropriate to evaluate cyber assets based upon accessibility and span of control. Therefore facilities such as Control Centers would be expected to contain multiple cyber assets that would be designated as high impact cyber assets. However, the cyber assets that are operated or managed from a Control Center would not necessarily be designated as high impact cyber assets, unless: 1. They have the ability to control other cyber assets or, 2. if, when destroyed, degraded or otherwise rendered unavailable: they could directly cause, contribute to, or create an unacceptable risk of- - BES instability; and/or - BES separation; and/or - a cascading sequence of failures. Or in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of- - instability; and/or - separation; and/or - a cascading sequence of failures; Or could hinder restoration to a normal condition. The current definition: “The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.” Is inappropriately overbroad, by including planning horizon. EEI suggests that the definition be modified to focus on time sensitive – real-time operations, e.g. “The Balancing Load and Generation function includes activities, actions and conditions necessary for monitoring and controlling generation and load in real-time.” In addition, elements of BES Cyber systems maintenance, such as change management are important, but should not necessarily be protected in the same manner as real-time systems operations.
O&R	Agree	

Organization	Yes or No	Question 6 Comment (Response page 18)
Alliant	Agree	See Question 12 for specific comments on Attachment 2 criteria.
Ameren	Disagree	The impact levels of high, medium and low associated with the BES Cyber Systems should also be evaluated with the high, medium and low impact level of their associated BES Subsystem and appropriate controls developed for the different combinations of categorizations of BES Subsystem & BES Cyber System as in the following matrix. BES Subsystem BES H/H M/H L/H Cyber H/M M/M L/M System H/L M/L L/L The effort to develop these nine different response levels initially would of course be higher up front but the granularity gained in this approach would allow for a more focused and efficient application of protection controls for the BES Cyber Systems identified.
Black Hills	Agree	
TNMP	Agree	TNMP agrees with the concept of assigning the highest impact level of the associated BES Subsystem to the BES Cyber System. However, the lack of clarity on the definitions of Cyber System and BES Cyber System mentioned earlier makes it difficult to determine exactly what the highest impact level would be applied to. Additional guidance, through definitions or other means, is needed to provide clarity or “bright lines” and improve this requirement. It may be necessary to create a requirement before this one or another criteria attachment giving guidance on how one goes about determine what makes up a BES Cyber System if the definition alone does not provide adequate clarity.
NVEnergy	Disagree	It is more appropriate to evaluate cyber assets based upon accessibility and span of control than by simply assigning the impact degree of the highest impact BES subsystem. For example, control centers are undoubtedly some of the highest impact BES subsystems under consideration; however, not all of the cyber systems within the control center carry that same level of impact. Hence, as suggested in comments above, the impact of the cyber systems themselves should be assessed first, then whether they are associated with a High Impact BES subsystem. Equally important, we urge the drafting team to acknowledge that the CIP security objectives should target only those cyber systems that are accessible via connections such as routable protocol, IP, and dial-up. Self-contained cyber systems, no matter their degree of importance, are not subject to the type of threat that the CIP standards have set out to address. Certain physical protections may be appropriate in these instances.
MWDSC	Disagree	See prior comments on lack of clarity in definitions and need for a "No BES Impact" category.
Empire	Disagree	I do not agree with assigning each cyber system the same level of criticality as the most impactful subsystem. Some cyber systems associated with a generating station, for example, do not impact the BES if disabled.
SWTC	Agree	If a common element roughly spans several facilities does this force all elements of those facilities to be high even if

Organization	Yes or No	Question 6 Comment (Response page 18)
		singularly they are low or medium. The way the standard is written it requires them to be high.
SCEG	Agree	
Exelon	Disagree	While we agree with the need to appropriately categorize and document BES Cyber Systems, we ask the SDT to consider including provisions for exceptions as well (e.g. non-routable protocol, lack of dial-up capability). As stated previously, Exelon is hoping for a timely and clearly stated scope of applicability from NERC and the NRC to U.S. nuclear plant generator owners/operators in order to provide a clear "bright line" to provide the needed guidance for implementation
BPA Trans	Disagree	1. This approach does not take into consideration how much the Cyber System can affect the Subsystem. A Cyber System whose loss, degradation, or compromise has only a minimal effect on a BES Subsystem could have very little impact on the BES, regardless of the Subsystem's impact on the BES. BOTH the impact of the Cyber System on the Subsystem, as well as the impact of the Subsystem on the BES, must be taken into account. 2. Using the methodology in the Standard could result in applying overly-stringent standards to Cyber Systems. To use a print server as an example, a Control Center print server supporting hardcopy reports could be construed as supporting Control & Operation as well as Situational Awareness. The lack of hardcopy reports could be construed to be an adverse effect on the Control Center. If the Control Center is of High impact on the BES, then so would be the print server. Yet, if the hardcopy is a last-ditch backup to online displays, the actual impact on the BES would be very small. Assigning a High BES impact to the print server would be inaccurate. A much better choice would be to determine the impact of the Cyber System on the Subsystem, in some manner that must be defined. In most cases, one could then limit the BES impact of the Cyber System to be no higher than its impact on the BES Subsystem it supports. With the addition of new requirement #1, the existing R3 becomes a new R4. Our changes to R4 are too extensive to be represented as edits to existing R3. Therefore, new R4 is rewritten in its entirety: R4. The Responsible Entity shall categorize and document BES Cyber Systems as follows: (Violation Risk Factor: High) R4.1. The Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R2, that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. R4.2. The Responsible Entity shall assign the BES impact categorization to each listed BES Cyber System which represents its potential impact on the BES Subsystem it supports. Where a BES Cyber System is associated with more than one BES Subsystem, the responsible entity shall assign the BES impact categorization level to that BES Cyber System that represents its highest potential impact to any of the associated BES Subsystems. The concept of greater and lesser security boundaries are not necessarily applicable in many utility situations. With this in mind, it is our opinion that the potential adverse impact of a cyber system on a BES Subsystem may not necessarily be significant enough that it would degrade the Subsystem(s) it supports, or the Bulk Electric System, enough to justify an

Organization	Yes or No	Question 6 Comment (Response page 18)
		impact of the level that matches that of the Subsystem itself. Cyber Systems should be graded on their own potential impacts on the subsystem(s) and the BES rather than simply being assigned the impact rating of the Subsystem(s) to them.
HQT	Agree	
Allegheny Energy	Disagree	We agree with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problem from CIP Version 1).
KCPL	Agree	With appropriate definitions and criteria for Attachments 1 and 2, these concepts should work.
Connectiv Energy	Disagree	Accomplishing 3.1 implies that an entity identify ALL cyber systems associated with each BES Subsystem and determine for each if it "has the potential to adversely impact any of the functions…". This is unnecessary for BES Cyber Systems that are associated with only LOW IMPACT BES Subsystems. Suggest modifying section 3.1 with a prefix similar to "For each BES Subsystem categorized as HIGH or MEDIUM impact, "
MidAmerican	Disagree	Change CIP-002-2 R3 to refer to the list of BES facilities (instead of Critical Assets). Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a “system.” Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls. Categorization level determinations should be addressed in the security control standards.
CPG	Disagree	Designating a cyber system impact solely on the impact of the BES subsystem is not a valid methodology in that it does not take into account the cyber system’s importance to the BES Subsystem. The current proposal may require an unimportant cyber system to be heavily protected for unnecessary reasons. Furthermore, R3.1 will require a listing of all cyber systems. This is not a worthwhile endeavor considering that many cyber systems are Low or No Impact for GO/GOPs. Listing only those cyber systems associated with High and Medium Impact subsystems is a far superior approach.
Santee Cooper	Disagree	While SC agrees that “one size fits all” is an incorrect approach to a standard, it seems as FERC is overtaxing the utilities to unnecessarily protect items that have no impact. Certainly, some assets have an impact to the utility and could cause inconvenience or local outages, but as a whole, if classified as FERC would like, would cause higher costs and higher rates for our customers.
OGE	Disagree	• In 3.1, the act of putting the Cyber System on the list makes it a BES Cyber System. Change this from BES Cyber System to Cyber System.

Organization	Yes or No	Question 6 Comment (Response page 18)
		• Every asset is High, Medium, or Low. There should be the option of some Subsystems being excluded, even from the Low Impact category. • We need some guidance for identifying the appropriate set of cyber assets. There seems to be no way to develop a "practical" list that makes sense without assessing the risk of all cyber assets.
Oncor	Disagree	The rationale for assigning of cyber security controls to BES Cyber Systems should recognize the real cyber threat of the cyber system to the reliability of the BES. The installation of a DFR in an EHV station does not necessarily have a “High BES Impact” and may not warrant “high” cyber security controls. We would support multiple levels (i.e., Low, Medium, High) to correspond with the appropriate level of cyber security controls and countermeasures appropriate for each cyber system.
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Disagree	The reference framework of electric grid engineering, facilities ratings, etc listed in Attachment 1 is not required and the alternative method sans the Attachment 1 criteria will be a better approach since the issues at hand needs to be approached from a networked-computing systems security engineering perspective. Hence, BES Impact Criteria in Attachment 1 should not be tied into.
MGE	Disagree	R3, “As a step in assigning appropriate security controls for its assets” should be deleted; the statement does not add content or instruction to the requirement. R3.1, Please clarify that only High and Medium BES Impact items are to be used in Attachment 2, since items listed in the Low BES Impact category do not have the potential to adversely affect the BES. R3.2, In order for R3.2 to have the maximum positive impact on assuring an adequate level of reliability, the Transmission Subsystem owner would also need to inform the Generator Subsystem owner the same information when a Transmission Subsystem is categorized as a High BES or Medium BES Impact for those Subsystems that are connected to each other.
FE	Disagree	FE believes that Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
TECO	Disagree	Please see our comments to question 2. As currently worded, this requirement introduces a one size fits all approach to any cyber system associated with a BES subsystem at a particular level. Cyber Systems that have a direct impact on BES subsystems, such as those with operational and control capabilities, should be assigned a higher impact and protected at a higher level than those that have an indirect impact, such as planning systems, change control, etc.. Consideration must be given to the criticality of the BES cyber system and its impact on the reliable operation of the

Organization	Yes or No	Question 6 Comment (Response page 18)
		associated BES subsystem. Not all BES cyber systems associated with a high impact BES subsystem should be subject to the same level of requirements. For example a planning system such as a load forecast system should not require the same level of security as a control and operation system such as a SCADA. Systems without direct impact should either be given a lower impact level or be removed from consideration as BES Cyber Systems. This requirement should have a sub requirement that gives a time length for updating the Cyber System list after an update to the BES Subsystems list in R1.1 (or the addition or removal of a Cyber System independent of an associated BES Subsystem). As the requirement states now, the Compliance Enforcement Authority could expect an update to the Cyber System list to be made simultaneous to the BES Subsystem list, which is not practical. Sub-Requirement 3.1: In categorizing each BES Cyber System based on Attachment 2, a number of systems may be included that may be significant from an operational stand-point but have very low probability in terms of actual threats. Versions 1-3 of CIP-002 filter Cyber Systems by use of “routable protocols.” Given the current state of potential threats in terms of cyber security, there are no measurable threats to proprietary architectures not using routable protocols. We should continue to use the routable protocol filter as a measure of probability in the risk analysis required in Requirement 3. It is not supported that a plant DCS controller communicating on a vendor specific proprietary protocols is as High Risk as one that communicates through TCP/IP. While both are operational significant, the actual threat probability is much lower for the proprietary system. It is not clear how cyber systems such as firewalls, network infrastructure, physical security controls, and environmental controls will be assigned a BES impact level.
CECD	Agree	1. The phrase "as a step in assigning appropriate security controls for its assets" should be deleted because the purpose of the standard has been stated. 2. Agreement is based on the registered entity having flexibility to define its BES Subsystems and the ability to appropriately identify the impact to the BES.
MRO	Disagree	We feel the introduction statement “As a step in assigning appropriate security controls for its assets,” adds nothing to the requirement and should be deleted. Otherwise, we agree with the method in principle, however, see answers to questions 12 for specific comments on Attachment 2 criteria.
GTC	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not consider the degree or type of risk associated with the BES Cyber System itself. We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will far outweigh its benefits.

Organization	Yes or No	Question 6 Comment (Response page 18)
		It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
Xcel	Agree	
BGE	Disagree	Regarding BES cyber asset categorization, we feel that cyber assets should be evaluated based upon accessibility and span of control of the cyber asset. Under the current approach facilities such as Control Centers would have multiple cyber assets designated as high impact cyber assets regardless of the asset's true potential to impact the BES. The cyber assets that are operated or managed from a Control Center should not be designated as high impact cyber assets, unless: 1. They have the ability to control other cyber assets or, 2. if, when lost, degraded or otherwise rendered unavailable: they could directly cause, contribute to, or create an clearly defined unacceptable risk of: - BES instability; and/or - BES separation; and/or - a cascading sequence of failures. Or in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of: - instability; and/or - separation; and/or - a cascading sequence of failures; Or could hinder restoration to a normal condition.
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	It appears that the revised standard does not provide a distinction between cyber systems that use a routable technology and those that are either completely isolated or connected through non-routable means (proprietary networks or layer 2 communication networks). Isolated Cyber systems should be considered a low risk and CIP-005 & 007 should not apply. In categorizing each BES Cyber System based on Attachment 2, a number of systems may be included that are significant from an operational stand-point but have very low probability in terms of actual threats. Versions 1-3 of CIP-002 filter Cyber Systems by use of "routable protocols."
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP agrees with the approach that some components of a shared BES cyber system should inherit the level of protection associated with the highest impacted BES subsystem; however we do not agree that all BES cyber assets should be

Organization	Yes or No	Question 6 Comment (Response page 18)
		treated equally within the shared BES cyber system (i.e. Server afforded the same protection as a printer or a network switch simply because they are used within the same BES cyber subsystem – continuation of the one size fits all problems from CIP Version 1).
FMPA	Disagree	FMPA recommends that the SDT either eliminate Attachment 2 or convert it to a reference/guidance document supporting the standard. The important criteria of the standard are included in Attachment 1. The conceptual discussion of functions in Attachment 2 only adds redundancy, complexity and confusion. If Attachment 2 identifies "functions critical to the reliable operation of the Bulk Electric System," there should be a one-to-one mapping of these functions to each of NERC's other reliability standards. Also, how are these functions different from those described in the Functional Model? Is Attachment 2 essentially another, different, functional model? At best, Attachment 2 should be treated as a list of "things to consider" when developing worst case scenarios/contingencies for evaluating the impacts of "unavailability, degradation or compromise" of a Cyber System. If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? Unless Attachment 2 is treated as a guidance document, the identification of reliability functions cannot be open-ended, implying that additional functions, or aspects of functions, have yet to be identified. The SDT should avoid open-ended statements such as: "Aspects of the Managing of Constraints include, but are not limited to" that are followed by a bulleted list. Further, the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. From this perspective, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is certainly NOT critical. Calculation of ACE is certainly NOT critical. This standard should focus on what is truly critical: threats of an Adverse Reliability Impact resulting in "instability, uncontrolled separation, or cascading" outage. If Attachment 2 is retained, FMPA suggests that it should be renamed: "Activities Performed to Maintain the Reliable Operation of the Bulk Electric System."
Duke	Disagree	We disagree, and prefer the "Cyber First" approach whereby Cyber Systems are first identified that can impact functions essential to BES reliability. Next, these Cyber Systems should be categorized based upon their risk and impact to the BES. For example, a system may represent LOW risk to its associated BES Subsystem facility, but could pose HIGH risk to BES reliability if it is attached to a routable protocol control system network.
NBSO	Agree	
AESI	Disagree	We feel that defining the impact level of a BES Cyber System solely based on the impact of an associated BES Subsystem does not provide an adequate basis for applying security controls commensurate with the potential impact of some BES Cyber Systems. We also disagree with the requirement in that when establishing the appropriate level of security controls it does not

Organization	Yes or No	Question 6 Comment (Response page 18)
		consider the degree or type of risk associated with the BES Cyber System itself. We believe that regardless of the method of assigning impact levels, it will be so complex to implement that its costs will far outweigh its benefits. It should be made explicit that an entity cannot be found in violation of R3 based only on a violation of R1.
IESO	Agree	
Manitoba 2	Disagree	All the devices or components in a BES Cyber System should not automatically inherit the categorization of the overall BES Subsystem. If many devices or components are part of the BES Cyber System, such as a plant control system, then the assessed impact could be Minimal (very low) for an individual device, such as a transducer. Redundancy (often mandatory requirements in other reliability standards) should be considered as it may reduce the impact of an individual BES Cyber System component. Redundant systems with different architecture or modes may require a lesser degree of security controls due to an inherent robustness, determined through a vulnerability assessment. Master ends of BES Cyber Systems may be categorized higher than the individual remote ends of the BES Cyber Systems, but no higher than the associated BES Subsystem.
ATC	Disagree	3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 6 Comment (Response page 18)</th></tr>
<tr><td></td><td></td><td>remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>PSE</td><td>Disagree</td><td>R3.2 causes concern as it potentially overly burdens Low impact cyber systems by association because of the concept of defaulting to the highest BES impact categorization level assigned. Smart Grid could bring more cyber systems into scope in the future and this requirement could have significant implications resulting in entities having to treat many Cyber Systems as if they have higher impact than they do simply by association with something else.</td></tr>
<tr><td>IMPA</td><td>Disagree</td><td>IMPA does not object to the requirement of assigning the highest impact level of the associated BES Subsystems, but we do have issues with Attachment 2.

Attachment 2 has issues in itself such as the definitions used to define functions critical to the reliable operation of the BES. For example under number six (Control and Operation), the definition includes activities such as actions and conditions that provide monitoring and control of BES elements. Elements should be deleted and replaced with BES Subsystems. An element may be a 138 kV potential transformer that’s used for local indication only. In addition an</td></tr>
</table>

Organization	Yes or No	Question 6 Comment (Response page 18)
		example aspect of Control and Operation is "All methods of operating breakers and switches (such as SCADA). What about manual operations?? Is the intent of this Standard to include any and all aspects of operating equipment?? If so then any station that has SCADA and has any equipment that can be operated either manually or remotely would have to be included and appropriate security controls applied. Attachment 2 also attempts to define "Situational Awareness" (number 8.) This is not a defined NERC Glossary Term so it needs to be defined. One of the aspects listed for the situational awareness function is "monitoring and alerting (such as EMS alarms)". This aspect would include every RTU installed in a BES facility. For example, Utility A may be interconnected at facility that is a High BES Impact facility. Utility A does not own, operate, or maintain the facility and their RTU may be used for "status only". But since the facility is High BES Impact then appropriate security controls would need to be put in place by Utility A for their RTU, even though the RTU is used for "status only". This could also apply to local indication, such a substation annunciator panel. Item 9 "Inter-Entity Coordination and Communication" could include all forms of communications such as voice, fax, and electronic (e-mail, text, etc.). This could potentially require the use of secure fax machines, secure voice lines, and encrypted electronic communications by smaller utilities when they communicate with a large Control Center that is determined to be a High BES Impact asset.
ERCOT	Agree	ERCOT ISO recommends that additional asset categories be addressed as well (i.e.: PSP, ESP, non-critical cyber assets, access control, monitoring, etc.)
PacifiCorp	Disagree	Change CIP-002-2 R3 to refer to the list of BES facilities (instead of Critical Assets). Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls. Categorization level determinations should be addressed in the security control standards.
PEPCO	Disagree	We believe that it is appropriate to evaluate cyber assets based upon accessibility and span of control. Therefore facilities such as Control Centers would be expected to contain multiple cyber assets that would be designated as high impact cyber assets. Please reference previous discussions.
NEI	Disagree	A) NEI is concerned with the approach of simply applying the BES Subsystem impact level directly to its BES Cyber Systems. The impact a BES Cyber System has on its BES Subsystem cannot be reduced through a cyber security program as it is a fixed variable. Reducing the threats or vulnerabilities to a BES Cyber System will reduce the risk to a BES Subsystem, and consequently the risk to the BES. Therefore, the evaluation of cyber security controls should be based on the risk a BES Cyber System poses to the BES as illustrated in the table shown during the SDT's August 25, 2009 webinar on page 13 of the slide presentation with the following adjustments: that the vertical access represent "Cyber System Risk" and the horizontal access represent "BES Subsystem Impact"; that a none category be added both vertically and horizontally with the resulting categorization being "none"; that High-Low and Low-High results in "Medium"; and that Medium-Low and Low-Medium results in a "Low." The resulting table outlines a graduated level for applying cyber security controls to BES Cyber Systems based on risk. BES Cyber Systems that have a low risk should not require the same cyber security controls as BES Cyber

Organization	Yes or No	Question 6 Comment (Response page 18)
		Systems that pose a high risk. Ratcheting the risk level to protect nearly everything will inadvertently result in a decline in the reliability of the BES. B) The size/rating of a "BES Subsystem" has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. A 69kV substation with a routable network link to its control host data center presents much higher adverse cyber security risk than an EHV substation served only by legacy serial communication lines to its control host. Pick any BES Subsystem and this fact remains the same. C) Attachment 2 as presented overly complicates the analysis required by industry. It is unclear how the team intends to use the information gained from the nine "critical functional classifications". We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Summary Consideration for VRF: Many respondents found it excessive for all requirements to have a High Violation Risk Factor. Some commented on the difficulty of assessing what was missed in the categorized BES Subsystems or Cyber Systems.

VRFs have been assigned to the redrafted requirements.

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
Progress Energy	Disagree	We don't believe that every subsystem should be categorized; only Facilities with High impact to the BES should have subsystems categorized. As new Facilities are added they would be evaluated and subsystems categorized if deemed a High impact Facility.
GSOC/OPC	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
SDGE	Agree	
APPA	Disagree	APPA Task Force Comments: The APPA Task Force believes that categorization of BES systems and subsystems are an administrative process and do not present a high risk to the BES. Therefore it should have a low VRF; however, improper application of security controls might increase the risk to the BES.
Consumers	Disagree	There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
NPCC	Agree	
SWPA	Disagree	
MPPA	Agree	
Central Lincoln	Disagree	Categorization does not equate to risk. The protection of the cyber equipment is what really matters, and might be sufficient regardless of whether they were categorized correctly or not categorized at all. Suggest Low for all requirements.
Dominion		Dominion could not locate the proposed VRFs in the review materials.
Encari	Agree	
US ACE – NW	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
SCE	Agree	
USBR	Agree	
Dyonyx	Disagree	Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Westar	Disagree	Should all be low.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE		No comment at this time
PSEG	Disagree	
WE-Energies	Disagree	Wisconsin Electric Power Company believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
Idaho Power	Agree	
SOCO	Disagree	
DTE	Agree	
AEP	Disagree	The requirements must be made much clearer in order to make the assessment of the appropriate level of VRFs.
Edison Mission	Disagree	Comments: Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Calpine	Agree	
NS&T	Agree	
Flathead	Disagree	There should be lower or no VRFs related to Low Impact assets.
E ON	Disagree	
Carthage		No comments
WECC	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
Entergy	Disagree	If the fundamental logic of the process is faulty from the very beginning (starting with R1 & R2 coupled with Attachment I) then any subsequent discussion of VRF/VSL validity is moot.
LCRA	Agree	
NIPSCO	Agree	Did not review proposed VRF's
ConEd		The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
EEI	Disagree	EEI believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
O&R	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
Ameren	Disagree	We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
Black Hills		Not thoroughly reviewed at this time.
TNMP	Agree	
NVEnergy	Disagree	A Medium VRF is more appropriate for the three proposed requirements. Failing to execute any of the three requirements does not in and of itself pose any risk to the BES. However, the accompanying security control standards, if violated, would pose a higher risk more suited for a High VRF assignment.
Empire	Disagree	
SWTC	Agree	
SCEG	Disagree	Did not find the VRF's in this document.
Exelon	Disagree	Exelon believes that the proposed Violation Risk Factors and Violation Severity Levels are overly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as the reference for version 4.
BPA Trans	Agree	
HQT	Agree	
Allegheny Energy	Agree	

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
KCPL	Agree	It is reasonable for the assignment of a HIGH VRF for applying appropriate criteria in the categorization of facilities and cyber systems within those facilities applying appropriate criteria.
MidAmerican	Agree	VRFs: The violation risk factor for R1 changed from medium to high while the VRFs for R2 and R3 stayed at high. MidAmerican supports these risk factors for the changes to CIP-002-2 proposed by MidAmerican as long as the criteria are clear.
CPG	Disagree	There need to be VRFs for TOs and RCs not providing information to GOPs as required in Attachment #1, Sections 1.1, 1.2, 1.3, 1.4, 1.6, 1.13, 2.1, and 2.5. Furthermore, it is hard to assess Violation Risk Factors when the draft versions of CIP-003 through CIP-009 have yet to be developed. A broader system view of how all of these standards are intertwined is needed.
Santee Cooper	Disagree	
OGE	Agree	
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Agree	
MGE		N/A
FE	Agree	We generally agree, with exceptions as stated above for R1.
TECO	Disagree	
CECD	Agree	
MRO		We'll withhold comments on these sections until the standard is more set.
GTC	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
Xcel		We'll withhold comments on these sections until the standard is more set.
BGE	Agree	No comments
Springfield, MO	Disagree	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Disagree	Since each entity will have different risk assessments we recommend that additional input from industry be provided when determining the VRFs.

Organization	Yes or No	Question 7 VRF Comment (Response page 19)
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes that moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.
FMPA		FMPA has many disagreement with the details of the requirements, therefore, we believe it is premature to comment on VRFs and VSLs.
Duke	Disagree	Requirements and associated VRFs need to be revised to the “Cyber First” approach.
NBSO		No comment
AESI	Disagree	We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case.
IESO	Agree	
Manitoba 2	Agree	
IMPA		IMPA has no comments.
ERCOT	Agree	
PacifiCorp	Disagree	VRFs: The violation risk factor for R1 changed from medium to high while the VRFs for R2 and R3 stayed at high. PacifiCorp supports these risk factors for the changes to CIP-002-2 proposed by PacifiCorp as long as the criteria are clear.
PEPCO		We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
NEI	Disagree	The VRFs wer not locatable on NERC site nor in CIP 002-4 as posted.

Summary Consideration for VSL: Some commenters noted that requirements must be made clearer to properly make the assessment of the VSLs. There were many specific suggestions for changes to the wording in the VSLs.

The SDT has redrafted the VSLs based on the substantially changed requirements in the new draft and on existing VSL drafting guidelines.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
Progress Energy	Disagree	We believe documentation required for compliance is unnecessarily burdensome and would not improve the reliability of the BES.
GSOC/OPC	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
SDGE	Agree	
Consumers	Disagree	It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty.
NPCC	Agree	
SWPA	Disagree	
MPPA	Disagree	R#1 Moderate VSL should specify 31 to 60 days, and high VSL should specify 61 to 90 days, and Severe VSL should specify greater than 90 days to remain consistent with R#2.
Central Lincoln	Disagree	Paradoxically, un-categorized BES subsystems or cyber systems must be categorized prior to VSL determination. Once they are categorized, the violation has been fully mitigated. If the regional entity is performing this assessment anyway, perhaps they should be responsible for all categorization under CIP-002 to avoid duplication of work.
NERC	Disagree	1. R2 – make the timeframes consistent with the expectations in R1. 30-40, 41-50, 51-60. We require the Responsible Entity to update the list in these timeframes but do not require the Generator Subsystem owner to report the change in like timeframes. 2. R3 – the VSLs have gaps. For example in the Lower level, there is no violation if 1-4 BES Cyber Systems have not

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		been categorized. There needs to be full coverage for all violations of the requirement to be consistent with NERC and FERC obligations. The other levels have similar issues. A remedy could be to assign impact levels based on the number of BES Cyber Systems not categorized (1 for Lower, 2 for Moderate, 3 for High, More than 3 for Severe)
Dominion	Disagree	Dominion disagrees with the VSL level determinations due to the ambiguity associated with the high, medium and low categories. No compliance violation should exist if an entity categorizes its assets in good faith and has supporting documentation for such categorization. Dominion suggests removing such criteria from the VSLs.
Encari	Agree	
US ACE – NW	Agree	
SCE	Agree	
USBR	Disagree	How will the number of "true" categorization or number of subsystems be determined as the basis of measuring what missed or miscategorized? This severity level determination is far too reliant on an external judgment. The measurement needs to be absolute an unambiguous.
Dyonyx	Disagree	Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Westar	Disagree	Severity levels should be adjusted to reflect the actual potential impact to the BES which in most cases will be low.
Oregon PUC		No comment
NB Power Gen	Agree	
Manitoba 1	Agree	
Portland GE		No comment at this time
PSEG	Disagree	Comment #1: It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty. Comment #2: There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
WE-Energies	Disagree	Wisconsin Electric Power Company believes that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		as a pattern for version 4.
Idaho Power	Agree	
SOCO	Disagree	
DTE	Disagree	We disagree with the severe VSL for R1. Failure to update documentation should not carry the same weight as not categorizing any BES Subsystems. Moderate VSL for R3 should reference BES Cyber Systems, not BES Subsystems.
AEP	Disagree	The requirements must be made much clearer in order to make the assessment of the appropriate level of VSLs.
Edison Mission	Disagree	Comments: Eliminate any need to specifically categorize Low Impact BES Subsystems and the associated VRFs.
Calpine	Disagree	Severity levels for R1 non compliance: Failure to update the categorization list should be changed to 30 to 60, 60 to 90 and greater then 90 days for moderate, high and Severe respectively. Low impact BES subsystems have no effect on the BES and should not be in the violation security levels. Remove R1. Lower VSL and R3 Lower VSL criteria. Further to comments made under question 5 on this comment form... The responsible entity should inform the regional entity under the deadlines specified. The regional entity will inform interconnected subsystem owners... R3 server VSL should drop firs criteria related to responsible entity it appears to be redundant. The severe violation should only entail ignoring the standard requirements.
NS&T	Agree	
Flathead	Disagree	
E ON	Disagree	Severe violation for failing to update BES categorization within 50 days after a change (R1.1) is too high. With respect to R3, if a non-affiliated BES subsystem owner fails to correctly categorize its BES subsystem leading the Transmission Subsystem owner to assign too low a categorization to its cyber systems, then it may lead the Transmission Subsystem owner to incorrectly categorize its associated cyber system. Assigning a severe VSL to the Transmission Subsystem owner under these circumstances is inequitable.
Carthage		No comments
WECC	Agree	
Entergy	Disagree	If the fundamental logic of the process is faulty from the very beginning (starting with R1 & R2 coupled with Attachment I) then any subsequent discussion of VRF/VSL validity is moot.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
CenterPoint		It is difficult to judge the VSLs because, as illustrated in our comments to question 8, it is difficult to define what the "subsystem" should be or how many "subsystems" exist.
LCRA	Agree	
NIPSCO	Disagree	It seems unreasonable to move from a Moderate - High - Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has mis-categorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty. Suggestion: Review the VSL / VRF details and remove the double time penalty option. Additionally, review the penalty equity between an entity who mis-categorized a BES subsystem and an entity who has not categorized any.
ConEd	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard. Failure to update the categorized list for a decommissioning of a BES subsystem being categorized and a high severity does not make sense. There is no exposure to any threats, so why would this be high severity?
EEI	Disagree	Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented, program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
O&R	Disagree	The penalties are much too large given the there is no history of established practices, there is judgment involved in interpreting the new versions of CIP standard.
Ameren	Disagree	We believe that the proposed Violation Risk Factors and Violation Severity Levels are improperly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
Black Hills		Not thoroughly reviewed at this time.
TNMP	Agree	
NVEnergy	Disagree	We disagree with the VSL's, particularly with regard to the high severity determination for the instance of missing or mis-categorizing only one BES subsystem. Given the degree of subjective judgment that is involved with the categorization, it seems inappropriate to assess such a severe violation level for what could amount to a disagreement between the Entity and the Auditor on the Impact of a particular BES subsystem. Perhaps the VSL's should be based upon the completion or failure to complete a categorization exercise itself.
Empire	Disagree	Severe violation for failing to update BES categorization after a change (R1.1) is too high. These are administrative in nature and provide no impact to the BES therefore they should be a low VSL.
SWTC	Agree	
SCEG	Agree	
Exelon	Disagree	Exelon believes that the proposed Violation Risk Factors and Violation Severity Levels are overly severe. Entities should not be subject to excessive compliance violations over disagreements in categorization. We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as the reference for version 4.
BPA Trans	Disagree	For R1, the VSL refers repeatedly to not categorizing a BES Subsystem of some impact level. Yet, without the categorization having taken place, how can the impact level have been determined? Also, the VSL refers to miscategorized Subsystems. Who determines that the Subsystem was miscategorized? Will the Regional Entities be performing their own independent categorization? R2. No comment. R3. This has the same issues as R1. How does an entity know the Impact level of a Subsystem that has not been categorized? Who makes the determination?
HQT	Agree	
Allegheny Energy	Disagree	It seems unreasonable to move from a Moderate to a High to a Severe simply due to a set period of time passing (10 days). The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed. It also seems unreasonable that an entity who has not categorized more than one BES subsystem or who has miscategorized it would receive the same severe penalty as an entity who has not categorized any BES subsystems. This seems to contradict the NERC stance on assessing an entity and utilizing mitigating factors when considering penalty.
KCPL	Disagree	The VSL's for Requirement 2 are based on the Registered Entity with generation to know their categorization level, which they may not be able to assess as explained in the response to question 5, so I think the VSL will need some additional work. In general, I struggle with the inclusion of the LOW in the VSL for Requirement 3 as if the reliability impact is LOW,

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		what is the point of a penalty considering the NERC concerns are preserving the highest levels of reliability impact.
MidAmerican	Disagree	VSLs: Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented; program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120); and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented; high-controls not implemented; moderate-reviews not completed; lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
CPG	Disagree	As written, a Responsible Entity will receive an increased VSL based on a time period, and then a higher penalty due to the length of time a violation existed. A severity level change should not be based on time, but rather another quantifiable measure. As for the VSLs for Requirement #3, a percentage of subsystems based on the entities cumulative total subsystems should be used instead of number of subsystems. That way, an entity with a lot of subsystems would be judged as fairly as an entity with a much smaller amount. Furthermore, it is hard to assess Violation Severity Levels when the draft versions of CIP-003 through CIP-009 have yet to be developed. A broader system view of how all of these standards are intertwined is needed.
Santee Cooper	Disagree	Every utility is different, with different impacts on their neighbors and the BES. The same mistake at a small utility would not have the same impact of a much larger utility.
OGE	Disagree	Miscategorized BES elements as a Severe VSL should not be warranted based any residual risk that might be present due to inadequate control sets.
PPL Supply	Disagree	Agree with EEI comments.
St. George	Agree	
NGRID	Agree	
MGE		N/A
TECO	Disagree	We support EEI's comments regarding proposed Violation Risk Factors and Violation Severity Levels. In addition, we offer the following suggestions for improvement. For R1, Lower VSL: By definition, Low Impact BES Subsystems have no impact on the BES, therefore they should not be listed under Violation Severity Levels. We suggest "One to three Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact." Then updating Moderate VSL to "Three or more Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact."

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		For R3, Lower VSL: By definition, Low Impact BES Subsystems have no impact on the BES, therefore they should not be listed under Violation Severity Levels. We suggest “One to three Medium Impact BES Subsystems have not been categorized or have been miscategorized as Low Impact.” For R3, Moderate VSL: Add “Cyber” after “BES.” Per the current R3 VSLs miscategorizing 1 or 2 Medium Impact BES Cyber Subsystems will NOT result in a violation. The suggested change to R3, Lower VSL above will solve this issue. For R3, Severe VSL: The last sentence states “The Responsible Entity does not have a list of ALL its BES Cyber Systems.” Technically this means if the entity misses listing even one of its Low Impact BES Cyber Systems they would have committed a severe violation. Suggest changing “all” to “any.”
CECD	Disagree	It appears excessive that 1 improper categorization of an asset is considered High, as does applying a Severe VSL for more than 1. Utilizing numeric values to change the VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems.
MRO		We’ll withhold comments on these sections until the standard is more set.
GTC	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
Xcel		We’ll withhold comments on these sections until the standard is more set.
BGE	Disagree	It appears excessive that miscategorizing an asset (see R1 under High and Severe VSLs) is considered “High” for 1 miscategorization and “Severe” for more than 1. Utilizing numeric values to change VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems, that is: should an entity that has a 1000 subsystems be penalized the same as an entity that has 10 subsystems when both miscatagorize 2 subsystems. Additionally, we feel that increasing the VSL every 10 days for a failure to update does not justify a change in severity level.
Springfield, MO		No comment at this time
FPL	Disagree	We disagree mainly b/c of the inclusion of low impact BES subsystems, as stated earlier.
TAPS		See TAPS response to Question 1.a.
Allegheny power	Disagree	AP believes that moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
FMPA		FMPA has many disagreement with the details of the requirements, therefore, we believe it is premature to comment on VRFs and VSLs.
Duke	Disagree	Requirements and associated VSLs need to be revised to the “Cyber First” approach.
NBSO		No comment
AESI	Disagree	VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here. The VSLs for R1 should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
IESO	Agree	
Manitoba 2	Disagree	The Violation Severity Levels appear inconsistent by equating a missed deadline for updating the categorized BES Subsystem list, with not categorizing any BES Subsystems under the Severe Violation Severity Level. All the deadlines for the VSLs should be 30 days, with differences based on impact level categorization. R1 Lower VSL should include “The Responsible Entity has failed to update its categorized list of Low BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the Moderate VSL should be changed to “The Responsible Entity has failed to update its categorized list of Medium BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the High VSL should be changed to “The Responsible Entity has failed to update its categorized list of High BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the R1 Severe VSL should be removed. The quantity thresholds used in the Violation Severity Level table should be a weighted score of an entity’s subsystems, where multiple Low BES Impact Subsystems or BES Cyber Systems are considered equivalent to single High Impact BES Subsystem or BES Cyber System, respectively.
LES	Agree	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable

<table>
<tr><th>Organization</th><th>Yes or No</th><th>Question 7 VSL Comment (Response page 19)</th></tr>
<tr><td></td><td></td><td>protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)</td></tr>
<tr><td>IMPA</td><td></td><td>IMPA has no comments.</td></tr>
<tr><td>ERCOT</td><td>Agree</td><td></td></tr>
<tr><td>PacifiCorp</td><td>Disagree</td><td>VSLs: Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented,</td></tr>
</table>

Organization	Yes or No	Question 7 VSL Comment (Response page 19)
		program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
PEPCO	Disagree	Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points.
NEI	Disagree	A) The requirements must be made much clearer in order to make the assessment of the appropriate level of VSLs. B) It is unfair to assess a penalty on categorization errors, given the vagueness of the terminology as noted elsewhere in the response.

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria?

Summary Consideration: Many respondents commented on the need to have the draft of requirements and controls available for review in order to comment. Commenters also wrote that criteria could be boiled down to two metric: supply/demand mismatch and exceeding IROLs.

Many comments questioned the basis of the bright line thresholds in the criteria. A number of comments questioned the use of gross nameplate values for evaluation of generation capability and cited the MOD-024 for rating of generation capabilities. One commenter stated that exceeding an IROL within the timeframe allowed by standards should not be High Impact. Commenters also questioned the use of the phrase "…leaving the station". Some entities asked whether Distribution Facilities supporting restoration and UFLS were in scope.

In formulating the thresholds and bright-line criteria, the SDT used many sources, such as the threshold in the NERC Event Analysis categories, and various thresholds used in existing standards.

The criteria are now used to categorize BES Cyber Systems based on their impact on the functions performed by BES Facilities. In consideration of comments, the SDT has revised, consolidated and removed various criteria in the former attachment 1. Most notably, the bright line criteria for generation are now based on defined terms in the NERC Glossary and used in standards MOD-024 and MOD-025. Criteria duplicative with IROLs have been restructured as options where IROLs are not used, and other criteria have been clarified and corrected where required. Periodic and time parameters have been added where there may be multiple criteria thresholds within a given time.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
Progress Energy	Need to have CIP003 through -009 Version 4 defined before we can respond appropriately. We request that CIP003 through -009 Version 4 be provided for review prior to the formal comment period.
Dynegy	1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a "Must Run" unit to add the following phrase at the end of the sentence: "that have wide area reliability impacts." 3. Add an Item in Category 2 that corresponds to Item 1.3 for "Must run" units that have "local area reliability impacts." 4. In Item 2.6., the word "controlling" needs to be clarified. This item should only encompass Control Centers and back up Control Centers that "remotely control and solely monitor the status of assets" rather than just performing redundant monitoring of those assets.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
GSOC/OPC	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
Hayden	As stated earlier in question 1.h the definition for "Medium Impact" is too vague and needs to be more specific to help the analyst figure out what the difference is between High and Medium impact and how to assign the impact level.
SDGE	• Define vague terms – For example, what is unacceptable risk, what is a “normal condition”, what does “directly affect the electrical state” mean? In order for the CIP Standards to be interpreted and applied equally across the industry, these terms need to be defined specifically or changed so that there is no ambiguity. • As mentioned above, we are advocating having two impact choices (High BES impact and No BES impact). We feel this makes more sense as we start to think about the other CIP Standards and the various requirements. We don’t want to have “high impact” and “medium impact” portions of the various requirements, as that would be too confusing to keep straight and implement successfully. • We feel that by including the “planning time frame criteria” in the “High Impact” and “Medium Impact” definitions, it adds a level of great deal of complexity to the process without a corresponding benefit to the reliability of the BES. • In the event that the SDT keeps the “planning time frame criteria” in the definitions, please define information such as study load levels, assumptions for line overloads (100% of applicable ratings, for example) to determine if cascading outages are possible. This is to ensure all parties are viewing reliability using the same consistent set of criteria. Further clarify cascading outages (we feel that loss of minimal load such as less than 100 MW should be low in impact). • If the drafting team declines to eliminate one of the high, medium, or low impact classifications, the drafting team should consider more operational definitions of high, medium, and low BES impact.
APPA	APPA Task Force Comments: Attachment 1 Criteria for BES Impact Categorization of BES Subsystems: High BES Impact (H): The APPA Task Force recommends that criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region). Bright line thresholds (such as 2000 MVA or 2000 MW) are useful default values that should be used in the absence of a particular BES design value used in a region for planning studies and real-time operations. The EPAct, FPA Section 215(a)(4) defines “reliable operations” as: “operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements," so, to

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	boil it down, the EPAct passed into law mandatory standards to regulate the industry in its efforts to avoid "instability, uncontrolled separation, or cascading failures" This definition of "reliable operation" is nearly synonymous with the NERC Glossary term for "Adverse Reliability Impact": "(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." "Cascading" is further defined by the NERC Glossary as: "The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies." The focus of the standard ought to use this concept of Adverse Reliability Impact to define what is High risk, Medium risk and Low risk. Supply/Demand Mismatch and IROL: Starting from this theoretical basis, what kinds of conditions can cause an Adverse Reliability Impact, such as widespread frequency related instability? The answer really is a large mismatch of supply and demand (even faults can cause instability by "shorting out" the load, causing a large mismatch of supply and demand) or operating conditions, regardless of cause, that lead to violation of an Interconnection Reliability Operating Limit (IROL). Therefore, the entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs. The rest of Attachment 1 is simply a restatement of conditions that can cause these metrics to be exceeded. IROL is defined in the NERC glossary as: "(a) System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." IROLs are determined by study by the PAs and TOPs and these metrics are readily available in accordance with FAC-014. Hence, the only metric that remains to be established is the supply/demand mismatch. This mismatch can be caused in a few ways: 1. Tripping a large amount of generation through malicious use of cyber systems 2. Tripping a large amount of load due to malicious use of cyber systems to directly trip the load (e.g., use of a large SCADA system to activate a centralized UFLS system). 3. Tripping key transmission Facilities by malicious use of cyber systems that could cause voltage instability, thermal cascading, etc., that could in turn result in a large mismatch of supply and demand, the large mismatch of supply and demand being the key. (For example, the Northeast Blackout of 1965 was caused by loss of tie lines importing power from Canada causing a large supply/demand mismatch, and the Blackout of 2003 was caused first by thermal cascading, which in turn caused a voltage collapse of Cleveland and Detroit, which then resulted in a huge supply /demand imbalance through the loss of two major urban centers) The APPA Task Force recommends that the SDT develop a metric for supply/demand mismatch (e.g., the Contingency Reserves of the region, or another metric determined by study) that correlate with High and Medium Impact. High Impact should include those events that have a relatively high chance of causing an Adverse Reliability Impact, e.g., cause an IROL to be exceeded or a supply / demand mismatch greater than a certain metric. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1000 MVA may be an acceptable default value in the absence of a specific regional threshold based on the largest single contingency for a PC or RC. Blackstart and Cranking Paths: If a cascade were to occur, utilities need to be assured that their blackstart units and cranking paths to other generators that are identified in the regional restoration plan will be available, and that the control systems for these devices have not been compromised. The Task Force understands the need for protection of the “critical units” and “critical paths,” but the identification of all blackstart units as High Impact is not reasonable or necessary to ensure BES restoration. APPA Task Force discussions indicate that that some of the Regional restoration plans were developed with different and inconsistent methodologies. There have been reports that some regions have just rolled up into their restoration plans all blackstart-capable units identified in each utility’s local restoration plan. This in effect designates all blackstart units as high impact in regions that are using this as a practice. The APPA Task Force recommends that the categorization of blackstart units and transmission cranking paths between the blackstart units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, “High Impact” from a restoration perspective should focus on preventing restoration efforts and “Medium Impact” should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent blackstart efforts from multiple blackstart units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder blackstart efforts from a single blackstart unit or cranking path in the regional plan. Blackstart capable units that are not in the regional plan should be Low Impact. Recommendation of Edited Language to High BES Impact (H): 1. High BES Impact (H) 1.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the Contingency Reserve or total Reserve Sharing Obligations of a Reserve Sharing Group or, if no Contingency Reserve or total Reserve Sharing Obligation has been established, a supply loss of 2000 MVA or a load loss of 2000 MW. 1.2. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.3. A BES Cyber System, that if maliciously used, can result in exceeding one or more Interconnection Reliability Operating Limits (IROL’s). 1.4. A BES Cyber System, that if maliciously used, can prevent blackstart restoration efforts from multiple black start units and cranking paths identified in the regional restoration plan. The APPA Task Force believes using the above criteria would make Attachment 1 very simple, resulting in only four criteria instead of the 16 in the "High Impact" list proposed by the SDT. Most of the 16 items in the "High Impact" list are simply phenomena that can cause supply/demand mismatch greater than the established metric, or an IROL to be exceeded (e.g., voltage collapse, thermal cascading, loss of situational awareness, etc.) We recommend including these phenomena as subsections of the four criteria spelled out above. We believe such a method is much simpler to understand and enforce, and is more in line with what ought to be regulated - phenomena that can cause an Adverse Reliability Impact. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	High BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC. Recommendation of Edited Language to Medium BES Impact (M): Medium Risk should be those events that would put the system dangerously close to an additional contingency causing an Adverse Reliability Impact, e.g., an event that could cause a supply / demand mismatch greater than the largest loss of source that would put the system in a status whereby a single contingency could cause a supply / demand mismatch greater than the Contingency Reserves of a reserve sharing group, or an IROL to be exceeded, (at a point only a single contingency away). Also, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 1000 MVA may be an acceptable default value for the Medium BES Impact threshold in the absence of a specific regional threshold based on the largest single source contingency. 2. Medium BES Impact (M) 2.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the single largest loss of source contingency of the region, or, if no single largest loss of source value has been established, a supply loss of 1000 MVA or a load loss of 1000 MW. 2.2. A BES Cyber System, that if maliciously used, can result in a system state whereby the next single contingency would cause the BES to exceed an IROL. 2.3. A BES Cyber System, that if maliciously used, can hinder regional blackstart restoration efforts by preventing blackstart from a single black start unit and cranking path identified in the regional restoration plan. Low BES Impact (L): Low Impact should include all other BES Cyber Systems that have a low risk of contributing to an Adverse Reliability Impact. The APPA Task Force cautions the SDT that even though the Low BES Impact category will have the least Adverse Reliability Impact, it will have the most burdensome and widespread impact on registered entities for compliance purposes. We cannot stress this point enough; the industry needs assurance that the Low BES Impact requirements will be reasonable. This category must be aligned with the cyber system protections that are programmatic in nature and are not cyber system specific. These requirements should be similar to the current CIP-002, which require a risk based assessment methodology where entities can manage compliance through employee training on the security of cyber assets, implementation of policies for the creation and protection of passwords, implementation of policies for access, etc. Making the compliance requirements exceedingly strict will take valuable resources away from the protection of the high and medium impact assets. The industry's first priority should be to protect and secure the high and medium impact facilities.
Consumers	Comment #1: Resolve the confusion of terms used in the proposed glossary additions. Comment #2: Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities' obligation. Comment #3: Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the aggregate load shedding capability or to the single step load shedding increment. Comment #4: There seems to be inconsistency in the use of MW vs. MVA Comment #5: We believe that the standard shouldn't use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement mod-024 Comment #6: We would like to understand the engineering basis for selection of MW criteria Comment #7: The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Comment #8: Nowhere in this proposed standard is it identified the benefit of the classification levels. Unless there are different security requirements specified for the different classifications, this is a meaningless exercise.
NPCC	Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. The detailed Attachment 1 definition does give clarification. In any system where the Contingency Reserve is less than 2000 MW, clause 1.2 dominates clause 1.1 so engineering evaluation cannot be used to reclassify a Generation Subsystem into having a Medium BES Impact. Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. Request clarification on the wording "leaving" in 1.5. Alternatively, suggest 1.5 be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station… Request clarification where 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include the distribution facilities necessary to complete the cranking path (facilities necessary to restore generation)? If 1.10, 1.11 and 1.12 should be removed and language added to 1.7 as follows: Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs) (or SOLs for those areas that do not identify IROLs), or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method. Request clarification on 1.13, which SPS 300 kV threshold (550 kV or higher for the Quebec Interconnection), sensing, action, or both? A SPS has a sensing portion and a portion that takes action. Sometimes these are not the same voltage, same station, etc. Also, 1.13 should be made to read: Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Request clarification on “automatic load shedding” in 1.14. If this refers to underfrequency load shedding then Distribution Provider must be added to the Applicability Section. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from “Each Control Center and backup Control Center” to “Each primary Control Center and any backup Control Center”. Request clarification on wording “leaving” in 2.2. Alternatively, suggest 2.2 be made to read: Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, 300 kV or higher for the Quebec Interconnection, or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines connected to the station… Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add “, including as notified by the Generation Owner”. Consistent with 1.9, recommend changing 2.4 from “NUC-001-1” to “NUC-001”. Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? A SPS has a sensing portion, and a portion that takes action. Sometimes these are not the same voltage, same station, etc. Alternatively, suggest 2.5 be made to read: Each Protection System, Special Protection System (SPS), or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, less than 550 kV for the Quebec Interconnection, or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. Consistent with the comment on 1.15 and 1.16, recommend changing from “Control Center and backup Control Centers” to “Primary Control Center and any backup Control Centers” in 2.6.
SWPA	Section 2.5: This section should include a lower voltage limit of 100kV for protection systems.
MPPA	The criteria for High, Medium and Low BES Impact should also be referenced by the definitions to maintain consistency. MPPA recognizes and concurs with the need for a multi-tiered approach.
Central Lincoln	1.1 There is no requirement for any of these entities to approve/disapprove assessments. 1.3 Pre-designated by who? 1.4 See 1.1 1.7 A huge burden. Simulations must be run for every individual bus and every individual line out of service? 1.8 This statement makes no sense. Including what? 1.10 See 1.7. 1.11 See 1.7. 1.12 See 1.7 2.1 See 1.1 2.2 See 1.1

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	2.3 See 1.1 3 See answer to 1.i. above. Please also see the APPA Task Force's suggestions on simplifying Attachment 2
TransAlta	Under High BES Impact section, item 1.2 states, "Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations". In the NERC "Security Guideline for the Electricity Sector: Identifying Critical Assets" approved by CIPC on Sept. 17, 2009, Page10, Table C-2, has the wordings for essential generation for the BPS (BES), specifically for the contingency reserve consideration. These two wordings are different. It is suggested that the draft team clarify item 1.2. Besides, the contingency reserve requirement in NERC BAL-002 standard applies to BA's, and the contingency reserve number may not be accessible by the generator owners/operators. As this criterion is written inside the draft standard right now, it will unduly put extra requirements for the generator owners/operators to get the contingency reserve from BA's . If the draft team want to keep it as a "bright lines" approach, then there should be some requirements in the standard which stipulate such data sharing among the different registered entities when performing the BES impact categorization.
NERC	1. Attachment 1 is overly complex and violates the intended outcome of "straightforward and objective". As stated previously, there is concern whether the Reliability Assurer or Reliability Coordinator has the available resources or desire to adjudicate Responsible Entity impact classifications and this would drive to eliminate this aspect of the criteria. 2. Part 1.2 – more specificity is required with regard to the timeframe of interest to identify the largest contingency reserve obligation. 3. Part 1.4 – reword to state "Each Blackstart Resource that has been included in a Transmission Operator's restoration plan per EOP-005. 4. Part 1.6 – reword to state "Each Transmission Subsystem that includes a Cranking Path used in a Transmission Operator's restoration plan per EOP-005. 5. Parts 1.10 – through 1.12 should be combined into one criterion for separation, cascading outages, etc. There is no meaningful distinction in separating the cause (e.g. frequency, voltage, or other collapse). 6. Part 1.13 – This criterion should be separated into two: one for Protection Systems for which the voltage distinctions would apply, and second for SPS and RAS for which the voltage distinction has no meaning. 7. Parts 1.13 and 2.5 – Eliminate Part 2.5 entirely. If the impact to the BES is the same, there can be no meaningful distinction between High and Medium. Therefore, modify 1.13 to remove the voltage classes, and remove the "Adverse Reliability Impact" reference and make consistent with the language used in Parts 1.10 – 1.12. 8. Part 1.16 – criterion should be separated into two: one for Balancing Authorities and one for Transmission Operators. For the Balancing Authority criterion, the language could read: "Each Control Center and backup Control Center performing Balancing Authority functions for load and generator exceeding 2000 MWs. For the Transmission Authority part, there is little relevance to the 2000 MW threshold. Therefore, it should be rooted in the transmission line delineations outlined in earlier criteria as follows: "Each Control Center and backup Control Center performing Transmission Operator functions for switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, or operated at 200 kV or higher in other Interconnections, with three or more

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	non-radial transmission lines leaving the station” 9. Medium Impact – modify the Protection System description in R2.5 with the less than 300 kV East and West, and less than 200 kV thresholds for others; modify the Balancing Authority and Transmission Operator control center criteria to use the 1000 MW threshold and similar voltage thresholds consistent with R2.2, respectively.
Dominion	Dominion suggests the following modification to the high category: High BES Impact (H) 1.2. Any Critical generating unit or plant whose aggregate output exceeds the value of the Contingency Reserve Requirement.
Encari	See comments made regarding definitions.
SCE	A “Not Applicable” or “No Impact” category should be added to the criteria.
USBR	It is not clear that the criteria proposed is necessary or consistent with the impacts described in the standard. 1.1. What was the basis for 2,000 MVA? Is it likely for the GO to perform the study that this refers to, or is it more likely to be by the TOP, Balancing Authority, Reliability Coordinator or the Reliability Assurer? None of whom are required to cooperate in such a study. 1.2. This requires the GO to have knowledge that the BA/TOP is not required to share. 1.3. What are these ”Reliability “must run” units”? These are not defined, so it leaves a question on what is meant, is this a marketing term that does not belong here? Is it referring to a Generator that must run for system reliability, whose loss or failure to operate will result in an Adverse Reliability Impact? 1.4. If there is not a Cranking Path defined to which the black start Generation Subsystem interconnects, it should not be required to have a high BES impact. 1.6. With no requirement to talk to your neighbor, the TOP could determine a Cranking Path which passes through one of our yards, and should be flagged as part of such, but we would have no knowledge thereof. This ties back to /R2, which says neighbor TO’s should also have to communicated High Medium with each other… 1.8. As there are no bilateral communications required the GO would not be aware of this situation. In addition, the phrase “including as notified by the Generation Owner” appears to be a back reference to the very standard which refers to this Attachment. 1.13. As currently worded, all SPS/RAS/PS would be exempt as none of these systems are operated at kilo-Volt level. They may protect systems that operate at that level. What are Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem? These are not defined.
Dyonyx	Attachment # 1 has many issues, a number of which have been presented in the paragraphs below according to their numbered paragraphs: 1.1 The arbitrary 2,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why “name plate MVA” rating has been designated versus “net output” based parameters.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1.3 Reliability "must run" units are frequently old units to be retired but held in an operational mode for MW capacity or VAR capabilities. Some regions are disbanding these unit designations. Accordingly, we do not believe that all "must run" designated units should categorically be included as High impact. 2.1 The arbitrary 1,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why "name plate MVA" rating has been designated versus "net output" based parameters. Lastly, we are not of the opinion that an interruption of this arbitrary value of generation necessarily will "directly affect the electrical state …..of the BES." For example, EROCT has a Contingency Reserve of 2,300 MW. The term "capability" of the BES is not an appropriate provision, e.g., the loss of even 10 MW will impact the total "Capability" of the regional system, but this is not the intent of the standard.
FMPP	Item 1.16 refers to CC performing BA or TO functions for transmission assets or generation assets of 2000 MW or more. What this sentence says is any CC with TO functions for transmission assets is High BES Impact. Transmission assets is lower case in this sentence so it is not defined. This sentence should be broken into two sentences one for BA and one for TO. How much transmission assets triggers a high impact should not use MWs, should use miles of 200kV and over or BES related or something related to TO. Item 2.6 does not refer to BA or TO. What this sentence says is any CC controlling transmission assets is Medium BES Impact. Again transmission assets is lower case so is not defined; also this sentence should be broken into two sentence one for BA and one for TO functions.
MISO	1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a "Must Run" unit to add the following phrase at the end of the sentence: "that have wide area reliability impacts." 3. Add an Item in Category 2 that corresponds to Item 1.3 for "Must run" units that have "local area reliability impacts." 4. In Item 2.6., the word "controlling" needs to be clarified. This item should only encompass Control Centers and back up Control Centers that "remotely control and solely monitor the status of assets" rather than just performing redundant monitoring of those assets.
Westar	Use the NERC defined term of Adverse Reliability Impact to categorize High Impact BES elements. Should replace the Low Impact Category with No Impact. The lack of routable protocol or dial up access should still be a consideration in the categorization level.
Green Country	I still would like to see a "No BES" Impact category.... exempt from CIP-003 thru CIP-009
Oregon PUC	Again, we recommend that the Low BES Impact level be eliminated.
Manitoba 1	Communication should be clarified, difference between dial up and LAN and the extent of the firewall. It is possible for banks to maintain firewalls so i think the level of the firewall would make a difference.
Wolverine	I agree conceptually with the categorization of assets into high, medium, and low BES impact. My concern is that what needs to accompany this draft in order for all to properly evaluate it, is a definition or proposal of what types and degrees of security controls would

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	accompany each category of asset. For example: Currently, if an entity determined through their RBAM that they have "no critical assets", then none of the controls and requirements of CIP-003 through -009 apply. Under this new proposal, let's assume the same entity would declare all assets to be "low impact". What type and level of security controls then apply to these "low" impact assets? None? (As per the old system?) Without information on the level of controls associated with this categorizing scheme, it is difficult to fully evaluate this concept.
Portland GE	No comment at this time
PSEG	Comment #1: Resolve the confusion of terms used in the proposed glossary additions. Comment #2: Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities' obligation. Comment #3: Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the aggregate load shedding capability or to the single step load shedding increment. Comment #4: There seems to be inconsistency in the use of MW vs. MVA Comment #5: We believe that the standard shouldn't use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement mod-024 Comment #6: We would like to understand the engineering basis for selection of MW criteria Comment #7: The distinction between High Impact and Medium Impact levels based on generation name-plate generation capacity has been set at arbitrary levels with no engineering basis. Also, basing any reliability standard on name-plate ratings is ridiculous. Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. Comment #8: Nowhere in this proposed standard is it identified the benefit of the classification levels. Unless there are different security requirements specified for the different classifications, this is a meaningless exercise.
WE-Energies	High BES Impact: • 1.2 a generator does not itself have a Contingency Reserve obligation or a RSG, MISO determines this and may vary as facilities may be out of service and the obligation may reduce. Moving target. • 1.3 needs to better define Reliability "must run", formal contract, reliability "out of market" dispatch (run our peaking generating stations for reliability now and again) could be moving target, or have Market implications. • 1.7 to include anything that a TLR would be called for is not High, should be Low if anything. • It's not clear under what conditions 1.7, 1.8, 1.10, 1.11 and 1.12 apply. We could create scenarios where the events described could occur, but would not reflect normal operating conditions we expect. This relates back to the inclusion of the "planning time frame" comments made earlier. For how many contingencies do we assess the impact?
Idaho Power	Attachment 1 of the proposed CIP-002-4 appears to focus on typical criteria that would be part of a system planning study. These studies

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	generally are based on N-1 and N-2 criteria which address only the loss of an asset(s), not the manipulation of the asset(s) thereby missing the point of Michael Assante's letter dated April 7. 2009 that states; "system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word "manipulate" here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new "cyber security" paradigm."
SOCO	In 1.1, the Regional Reliability Assurer is only defined in the Functional Model version 4, which is not approved yet. Also, NERC has issued a SAR to modify the NERC Glossary of Terms (issued 1-22-10 and comments due on 2-22-10) and this new Assurer is not shown in this modification either. We suggest just allowing the Reliability Coordinator for your region or subregion to be the approver. In 1.3, it describes listing "pre-designated as Reliability must run" units as a High Impact. In many large systems, this list of must run units changes on a daily basis, often for maintenance work in the area or even voltage support at various times. Since this would require an update every day, we suggest making only the "permanently assigned" units be on this list. A general note about the use of engineering analysis. It should be recognized by the drafting team and NERC staff that some conditions cannot be discovered without the use of an engineering analysis. For example, in 1.7, IROL's and TLR's are found by using studies in either the Planning time frame or the Operating time frame. Similarly, in 1.10, 1.11 and 1.12, voltage collapse, frequency related instability and cascading outages are all typically recognized in either the Planning time frame or the Operating time frame using engineering analysis. Therefore, in 1.1and 1.5, the drafting team and NERC staff should recognize that the same engineering analysis should be deemed credible when excluding generation and transmission subsystems that do not have an impact on the BES reliability when they are outaged. In 1.4, some very large systems have many blackstart units with multiple paths to multiple units it can start up. This makes no sense to protect them all and could be a waste of resources. Attachment 1, section 1.5 – Recommend that this definition be removed entirely or moved to the Medium Impact section; loss of individual Transmission Subsystems simply because it is above a specific voltage level does not cause BES instability, separation, or cascading failures. In 1.6, when discussing cranking paths, we suggest that 1.6 be moved to be next after 1.4, when discussing blackstart generation, if indeed the intent is to relate blackstart units to the cranking paths to some designated generation. Attachment 1, section 1.6 – a large utility with multiple blackstart units has multiple options for Cranking Paths; recommend that this definition be moved to the Low Impact section. In 1.7, by the definition of subsystems at the beginning of the document, this would potentially place ALL substations and generating plants in the High Impact category regardless of the system configuration. There are certainly those assets that this would be true for, but the majority of the time, we can do without almost ANY element. Attachment 1, section 1.13 – This definition basically includes all Protection Systems and Special Protection Systems operated at 300kV and above that if unavailable would have an Adverse Reliability Impact. Could not find a definition for "Adverse Reliability Impact". We assume Adverse Reliability Impact to mean risk of instability, separation, or cascading failures per the High BES Impact definition. Per the NERC Glossary of Terms, Protection System is defined as "protective relays, associated communication systems, voltage and current

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	sensing devices, station batteries, and DC control circuitry". Recommend Protection System be removed from this definition; loss of a Protection System simply because it is above a specific voltage level does not cause BES instability, separation, or cascading failures. Recommend "Special Protection Systems" be changed to "non-redundant Special Protection Systems". Also, suggest replacing "would have an Adverse Reliability Impact" with "would have an immediate adverse Reliability Impact such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures". Attachment 1, section 2.2 - Recommend that this definition be removed entirely or moved to the Low Impact section; loss of individual Transmission Subsystems simply because it is above a specific voltage level does not affect the capability of the BES. Attachment 1, section 2.5 - This definition basically includes all Protection Systems and Special Protection Systems operated at less than 300kV that if unavailable would have an Adverse Reliability Impact. Could not find a definition for "Adverse Reliability Impact". We assume Adverse Reliability Impact to mean risk of instability, separation, or cascading failures per the High BES Impact definition. Per the NERC Glossary of Terms, Protection System is defined as "protective relays, associated communication systems, voltage and current sensing devices, station batteries, and DC control circuitry". Recommend Protection System be removed from this definition; the current wording would cause all protective relays operating at less than 300kV and above 100kV (per definition of Bulk Electric System) to be in scope without any regard to a real impact on the BES. Also, suggest replacing "would have an Adverse Reliability Impact" with "would have an immediate adverse Reliability Impact such that subsequent contingencies may cause BES instability, separation, or cascading sequence of failures". The term "aggregate" is not defined in Attachment 1. For plants with multiple units this would imply that the combined output of all units should be considers as a single Generation Subsystem. There is no delineation for consideration of units, which are not interconnected by common cyber systems. This delineation should be included. Consideration should be provided to allow a Generation Subsystem to be classified as either a Medium BES Impact, Low BES Impact or a proposed No BES Impact system where supported by the identified evaluation or assessment method. Rational for the threshold values of 2,000 MVA and 1,000 MVA should be provided to assist in the analysis. Consideration should be provided to allow a Generation Subsystem to be classified as either a Medium BES Impact, Low BES Impact or a No BES Impact system where supported by an engineering study. Blackstart units are required to start during periods without available offsite power, this would most likely preclude the use of cyber connectivity. The requirement that the connectivity not constrain operation is probably better covered under another reliability standards scope. Attachment 1 Criteria 1.8 states "including as notified by the Generation Owner." Should this be "as notified by the Generation Owner."?
AEP	The functional approach for determining impact categories would provide the opportunity to clearly define what is most important and what needs the greatest attention. It's important to recognize that most any system is designed to continue to operate successfully, even under conditions where some parts are not optimally functioning. The factor of how long can you continue with without certain components helps to prioritize the protection necessary. Also, many systems contain algorithms to address fault conditions and back-up components for failed occurrences. These factors don't seem to come into consideration under the current draft standard approach.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
Edison Mission	Attachment # 1 has many issues, a number of which have been presented in the paragraphs below according to their numbered paragraphs: 1.1 The arbitrary 2,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why "name plate MVA" rating has been designated versus "net output" based parameters. 1.3 Reliability "must run" units are frequently old units to be retired but held in an operational mode for MW capacity or VAR capabilities. Some regions are disbanding these unit designations. Accordingly, we do not believe that all "must run" designated units should categorically be included as High impact. 2.1 The arbitrary 1,000 MW name plate rating parameter does not appear to be appropriate for all regions. We are confused as to why "name plate MVA" rating has been designated versus "net output" based parameters. Lastly, we are not of the opinion that an interruption of this arbitrary value of generation necessarily will "directly affect the electrical state …..of the BES." For example, EROCT has a Contingency Reserve of 2,300 MW. The term "capability" of the BES is not an appropriate provision, e.g., the loss of even 10 MW will impact the total "Capability" of the regional system, but this is not the intent of the standard.
Calpine	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
NS&T	We believe criteria should be simplified in order to avoid having the process of identifying high, medium, and low impact BES assets consume excessive amounts of time and effort.
Flathead	Eliminate Low BES Impact assets as by definition they are not critical. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at small LSE/DPs that didn't identify critical assets. The low impact methodology has the potential to affect small entities more than the ones this re-write should properly target.
E ON	The drafting team should clarify item 1.5 of Attachment 1. Does the 3 line criteria only apply to 300kV and above or any voltage transmission line. For example, would a substation with 345kV looped in and out and one 138kV line exit qualify as a "High BES Impact" asset? Similar comment for item 2.2 under Medium BES Impact.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Also, Using TLR as a criteria for classifying a Transmission Subsystem as High BES Impact seems overly restrictive. TLRs are called for a variety of reasons (planned outages, unforeseen loop flows, weather impacts, etc.) that do not seem to be a very good indication of the criticality of an asset. The criteria of IROL as stated is the only criteria needed in item 1.7.
Carthage	Make sure that the criteria are as specific as possible to eliminate confusion. No specific comments for High BES Impact. Section 2.5 under Medium BES Impact states that Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300kV in the Eastern and Western Interconnections, or less than 200kV in other interconnections that have an Adverse Reliability Impact. CWEP feels that simply stating each protection system, special protection system or remedial action scheme operated at less than 300kV is too broad a range. We feel that this could be interpreted to mean every piece of protective equipment operated at less than 300kV including protective relays and other equipment on our distribution system that have no material impact on the BES. CWEP offers the following revision to 2.5 for consideration. Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated from 100kV to 299kV in the Eastern and Western Interconnections, or 100kV to 199kV in other interconnections that have an Adverse Reliability Impact. CWEP feels that there should be criteria established for Low BES Impact and a category of No BES Impact added. CWEP has facilities that it feels should be evaluated in the categorization process but would not fit under any of the criteria established for High or Medium Impacts. We further feel that simply placing them in the Low Impact category because they don't fit in the High or Medium categories wouldn't be correct because they don't have any material impact on the BES. CWEP feels that not having a No BES Impact category would create a situation where entities leave facilities out of their assessment so that they don't have to implement any controls on those facilities.
WECC	see previous comments about ambiguity and passive language.
Entergy	Apply them appropriately. Hierarchical categorization of loss impact of individual electric operating sites/assets may be useful in defining physical security standards. But electric grid asset rating/size categorization is not salient to definition of hierarchical security control and countermeasure requirements for cyber assets. Hierarchical sets of requirements (controls and countermeasures) are needed for cyber assets themselves, based upon how much risk they themselves pose to reliable operation of the bulk electric system should they be lost or compromised.
CenterPoint	In Item 1.5, one sees the implementation problem introduced by the "BES subsystem" classification. Since the entire Eastern interconnection is interconnected, for example, all 345 kV facilities and higher could be considered a Transmission Subsystem under 1.5. If this subsystem were "destroyed, degraded, or otherwise rendered unavailable", the BES would most certainly be unstable. The net effect of such an interpretation, which fits the definition of transmission system and the verbiage in 1.5, would be that every transmission asset rated 300 kV or higher in the Eastern Interconnection would be considered a "Critical Asset" or "High BES Impact" subsystem because it is part of the High Impact subsystem. Although the Eastern Interconnect is used as an example, the same result would be true for WECC and ERCOT. One could certainly argue that the entire system is by definition not a "subsystem". The question then becomes how much of the system should be considered a "subsystem"? Would all of FP&L's 300 kV and above facilities be considered one "subsystem"? Or would all 300

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	kV and above facilities in the state of Florida be one “subsystem”? Or all 300 kV and above facilities in SERC be one “subsystem”? Or is it somewhere in-between these illustrative examples? The point of this discussion is that the verbiage indicating facilities above 300 kV or 200 kV would not be considered “high impact” if an engineering evaluation indicated loss of the subsystem would not cause instability or voltage collapse appears to either be a red herring (because all such facilities could be part of a large enough “subsystem”) or lead to differing opinions as to when a subsystem is too big to be considered one single subsystem. For this reason, CenterPoint Energy re-urges classification by asset, not by the proposed “subsystem” classification that is open to varying interpretations. Besides the rather large flaw discussed above in 1.5, which could be remedied by changing “subsystem” to “asset”, item 1.5 also appears to have an arbitrary and inexplicably discriminatory distinction of 300 kV versus 200 kV facilities for the Eastern and Western interconnection versus other interconnections. CenterPoint Energy operates in the region that is the apparent target of the discrimination, ERCOT. Ironically, the distinction between 200 kV and 300 kV facilities within ERCOT does not matter because no transmission facilities operate in that range in the ERCOT region. Nevertheless, CenterPoint Energy encourages a non-discriminatory requirement, either at 200 kV or 300 kV. Items 1.4 and 1.6 are either overly broad or unreasonable. As the discussion of item 1.5 illustrates, the interconnected nature of the BES allows everything in it to arguably be construed as a “subsystem” and any subsystem at some point will be large enough to cause the failure of the entire system. In such a paradigm, creating “impact” based distinctions becomes meaningless and open to differing interpretations. The present standard requires consideration of black start units and assets within cranking paths. If a region has significant diversity of black start resources and diverse cranking path options for each resource, it is possible that any single, independent (no common element or cyber system with another black start resource) black start resource would not be “critical” or “high impact”. Even if all black start resources are considered critical, a valid risk-based assessment would consider the diversity of cranking paths to ascertain whether assets in any given path would be “critical” or “high impact”. The wording in 1.6 indicates all possible cranking paths would be high impact, which conceivably could be all or most of the network, yielding an illogical outcome. For example, a black start unit with three different cranking path options has many more options and is therefore more secure than a unit with only one cranking path. The facilities associated with three different cranking paths are much less critical and have much lower impact if damaged than the facilities associated with one single cranking path. However, ironically, many more assets would be classified as “high impact” or “critical” under the scenario where there are three available paths than the scenario with only one path, a completely illogical result. At a minimum, CenterPoint Energy recommends revising 1.6 to criteria based upon diversity of cranking paths, such as designating as cranking path assets as critical until a threshold number of different paths are available, such as two or three. CenterPoint Energy recommends deletion of 1.7. This criterion diverges from the alleged definition of high impact facilities. Violating an IROL is a different standard from the criteria of instability, cascading outages or voltage collapse. Applying 1.7 would cause all or virtually all facilities to be considered high impact, negating the exercise of attempting to distinguish high impact or critical facilities from other lower impact, less critical facilities. CenterPoint Energy also recommends deletion of 1.9. Certain facilities may be pertinent from the standpoint of providing, say, off-site power to a nuclear power plant, but such facilities may not have a significant BES reliability impact. Moreover, NUC-001 requirements relating to concepts such as maintaining steady state switchyard voltage in a certain range would be open-ended if put into the context of proposed item 1.9 because voltage at a nuclear plant interconnection switchyard depends upon the cumulative effect of the entire transmission network and the generators connected to it. NUC-001 is specifically designed as the appropriate standard to address such

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	issues, not CIP-002. Indeed, to the extent that certain aspects of CIP-002 might be relevant to certain aspects of nuclear plant operations, the nuclear plant operator can address the issue by providing the applicable reference to CIP-002 through a Nuclear Plant Interface Requirement as outlined in Requirement R1 of the NUC-001-2 standard.
LCRA	1. Attachment 1, 1.4 – This is not clear. Does this only include the primary blackstart units or does it extend to any unit mentioned in the plan for any reason? 2. Attachment 1, 1.5 – This needs to be more clearly defined. The three or more transmission lines leaving the station need to be defined as also being operated at or above the 200 or 300 kV voltage levels. 3. Attachment 1, 1.6 – The current definition of cranking path in the Glossary is too general to be used in this statement. The sentence would better define the path as follows: “Each Transmission Subsystem comprising the primary Cranking Paths between the primary blackstart units and the next start units.” 4. Attachment 1, 1.16 – What is the definition of “transmission assets of 2,000 MW or more”? Does this mean transmission serving 2,000 MW of load or transmission lines capable of carrying 2,000 MW of power? 5. Attachment 1, 2.2 – This needs to be more clearly defined. The three or more transmission lines leaving the station need to be defined as also being operated at or above the 100 or 200 kV voltage levels.
FRCC	The use of the term "degraded" is used in many of the identified assets (1.7,1.10,1.11, 1.12 and more). As previously mentioned, this term can mean many different things and it will likely result in interpretation requests. The drafting team should try to be clear what impact they really want to be considered and be specific in the language.
NIPSCO	Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities’ obligation. Item 1.14 refers to the BES Subsystem that performs automatic load shedding of 300 MW or more. It is not clear if this refers the aggregate load shedding capability or to the single step load shedding increment. There seems to be inconsistency in the use of MW vs. MVA We believe that the standard shouldn’t use nameplate rating, but should be using Net Demonstrated Capability (NDC) requirement similar to MOD-024-1
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A-10 Criteria. Also it is recommended the standard raise the requirement of the 300 MW of automatic load shedding. This value should be 500 MW.
EEI	Proposed amendments to Attachment 1 were provided earlier.
O&R	NERC should consider that certain entities may have facilities that fall under the BES definition for a given region, but because of their own system's characteristics, do not have an impact on the Interconnected BES. There should be an additional category of NA, as with other NERC Reliability Standards. Since the NERC standards apply as per the entity's registration, the entity would then need to provide

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	evidence as to how they categorized the BES subsystems. If all/any BES subsystem elements that are not High or Medium are simply categorized as low, depending on what requirements CIP-003 - 009 bring forward, there could be undue and unjustified entity/consumer costs associated with implementation on BES elements that really do not require such. The Drafting Team should consider use of an impact-based methodology such as the NPCC A-10 Criteria. Also it is recommended the standard raise the requirement of the 300 MW of automatic load shedding. This value should be 500 MW.
Alliant	We believe Item 1.2 should include "for the Contingency Reserve Sharing Group" at the end of the statement to make the intent clearer. In Item 1.2, the term "Reserve Sharing Obligations" should be defined in the NERC Glossary of Terms. In Item 1.3, the term "Reliability must run units" should be defined in the NERC Glossary of Terms. Under Item 1.4, we believe this represents the same "one size fits all" approach that the Guidance for the Electric Sector: Categorizing Cyber Systems document claims to be trying to eliminate. In reality, not all blackstart Generation Subsystems listed in the Regional Restoration Plan carry the same weight, or have the same impact on the region, so it seems like a hierarchy should be developed within the standard for categorizing these units as either High, Medium, or Low Impact. We feel this hierarchy should be based on the size of the Generation Subsystem (similar to the delineation defined by CIP-002-4 Attachment 1, Sections 1.1 and 2.1, but not at the same MVA level), as well as the Generation Subsystem's impact on the Regional Restoration Plan, such as if it has a role in cranking support for a nuclear plant. Item 1.4 does not differentiate between a utility having numerous blackstart capable Generation Subsystems, where failure of multiple blackstart Generation Subsystems would not compromise their entire blackstart plan, or a utility with a single blackstart Generation Subsystem that is then essential to the success of their blackstat procedure. A utility should be given consideration for having multiple blackstart Generation Subsystems, which makes their blackstart plan inherently more reliable, not penalized for it. In Item 1.10 we propose to replace "in voltage collapse" with "in voltage collapse that would pose and unacceptable risk to the Adequate level of Reliability to the BES. In Items 1.16 and 2.6 we do not believe transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
Ameren	1.1 Deliverable MW should be used rather than the nameplate MVA for the generation subsystem. 2000 MW is an appropriate threshold for the high BES impact. 1.3 Generators designated as RMR to prevent IROL or are needed to prevent the loss of over 300 MW of load should be included as "high". RMR generators that are needed to prevent loss of load of less than 100 MW should be considered as low BES impact, and for loss of load of 100 to 300 MW should be classified as medium BES impact. 1.4 Only the black-start generators that are in the Regional Restoration Plan and are integral to system restoration should be candidates for high impact. Other black-start units should be considered as medium impact. Use EOP standard for criteria for system restoration.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1.5 Use criteria from EOP for system restoration so that all black-start units and all cranking paths are not considered high impact. 1.6 All transmission substations in all Cranking Paths do not qualify for high impact. Only those substations in Cranking Paths that are integral to System restoration should be included as high. The substations in other Cranking Paths should be considered as medium or low. Use EOP standard for criteria for system restoration 1.7 Remove “or exceeding limits requiring transmission loading relief (TLR)” 1.8 Remove “including as notified by the Generator Owner” Remove 1.10, 1.11, and 1.12 1.13 Added language “associated with” after “each protection system” 2.1 Similar to 1.1 above, deliverable MW should be used rather than the nameplate MVA for the generation subsystem. 1000 MW is an appropriate threshold for the medium BES impact. 2.3 This statement should be modified to replace section 2 with section 2.1. 2.5 Our view of this language makes all Protection Systems of less than 300 kV as medium impact. SPS that pass TPL-003 and TPL-004 requirements should not be included.
Black Hills	In Attachment 1, Section 1.2 on RSG obligations - need clarification of whether 'obligation exceeded' refers to that required by a single entity, or the total of all entities in the RSG. For consistency, the impact evaluation of a BES Subsystem be done by an RC.
TNMP	The criteria needs to have a means of addressing jointly-owned BES Subsystems, as mentioned in the comments for number four regarding requirement R1. Another significant concern is the requirement for engineering studies called for in the High Impact. To successfully pass an audit, a Responsible Entity would need to perform engineering studies on all Transmission Subsystems. TNMP sees this approach as casting too wide a net with little incremental return. TNMP believes the engineering studies in 1.10 through 1.12 should have the following constraints: -A Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections with 3 or more transmission lines leaving the station. -Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in the loss of a Generation Subsystem defined in CIP-002, Attachment 1, section 2, Medium BES Impact. -Excluding any Transmission Subsystem that has already been identified as High Impact based upon other matching criteria. These constraints would limit the scope of studies to determining if a Medium BES Impact station should actually be a High Impact. It also eliminates the need for engineering evaluations being performed for compliance purposes on stations that are already defined as having a High Impact.
NVEnergy	Suggestions for improving proposed criteria: Comments on specific sub-items as indicated below:

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1.1 The 2000MVA threshold appears on the surface to be a reasonable breakpoint for designation as High Impact; however, the use of a fixed value may not adequately account for the relative sizes of various Balancing Areas and Interconnections. 1.2 This item could use some additional clarity. What does it mean to have output that exceeds the Contingency Reserve or total Reserve Sharing Obligations? Obligations of whom? As an example, if a BA has an obligation share to its reserve sharing group of 75MW in a particular hour, does that imply that any generating unit larger than 75MW is High Impact? This is out of line when compared with the 2,000MVA level indicated in 1.1. 1.3 For Reliability Must-Run unit designation, the standard must clarify that the reliability scope is of the BES, not the local distribution, for instance. Also, it is unclear who would make such designation. 1.4 As noted in response to #2 above, the importance and criticality of Black Start facilities are being over-stated by placing them in this category. 1.5 Clarity is needed in the definition of transmission lines. Does this term include only the elements that function as transmission lines, or does it also include radial feeds, station positions that interconnect generator step-up transformers, or other transformer connections? What is driving the threshold of 3? 1.6 As with blackstart generators, the inclusion of the Cranking Path facilities in this category is inappropriate. 1.13 More precision is needed in this language, which currently categorizes Protection Systems, SPS or RAS “operated at 300kV and above” as High Impact. None of these systems operate at high voltage; what was intended was to refer to the BES systems that they protect operate at 300kV and above. As well, how does an entity determine if the destruction of such SPS would have “Adverse Reliability Impact”? What degree of impact is allowable? 1.14 A departure from the CIP-002-1,2,3 Standards in this version 4 removes the qualifier that the 300MW load shedding system is under a common control. Is this language intended to capture discrete underfrequency load shedding relays that are sprinkled throughout an entity’s distribution system? If so, this reaches too far. 1.16 The size threshold of system controlled by a BA/TOP control center is proposed at 2,000MW. Is this value a transmission capacity number, generation capacity number, or total system/area load value? If load, is it the historical peak, forecast peak, average over the peak season, other?
MWDSC	If an engineering evaluation demonstrates no Adverse Reliability Impact of any interconnected BES, add another category such as "No BES Impact" or a subcategory of Low BES Impact with limited application of unknown security requirements in CIP-003 through CIP-009. Add a guideline at the same time as standard is completed such as Table C - Evaluation Guidance of NERC's Guideline for Identifying Critical Assets, Version 1.0, dated September 17, 2009.
Empire	Need to show Bright lines. Black start units are defined differently in different regions. The RC should determine who's BS unit has a high impact on the BES based on RC study. Merely listing a unit as a BS unit does not necessitate it as a high impact to the BES. For example some BS units can be a 5kw gas engine in a metal shed and another’s may be a 20MW CTG or a hydro unit in a dam, yet all would, according to the proposed standard have the same High impact to the BES and this seems wrong in nature. It would be best for the RC to determine these High impact BS units based on regional studies to what is important for the region. People with multiple blackstart units are tempted to remove those from the current regions plan in order to be compliant with the proposed standard, hence undoing

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	reliability of the BES in order to show compliance with the standard. A different approach is needed.
NCEMCS	As stated many times "Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009, or a category for minimal-risk or no-risk subsystems must be created!"
SWTC	There is not much in the proposed standard that provides sufficient guidance on how to designate a transmission or generation subsystem. The emphasis appears to be mostly on determining whether the transmission and generation subsystems - to the Bulk Electric System (BES) - have a high, medium, or low impact. Attachment 1 to the proposed CIP standard tries to set some guidelines for transmission and generation for high and medium BES impact, but then lump the rest into the low BES impact.
SCEG	Beneath the Impact level categorization items should be more clearly grouped based on subsystem type. The SDT should also define Protection Subsystems.
Exelon	As stated previously Exelon supports the use of Attachment 1 as the primary tool for the categorization of system/subsystem elements. We ask that the criteria listed in attachment 1 be evaluated and revised to remove any ambiguity and technical justification be considered as a primary factor for setting the criteria.
BPA Trans	Suggestions for improving proposed criteria: This needs to be simplified. All of the criteria (1.7, 1.8, 1.10, 1.11, 1.12, 1.13, and 2.3) that includes the statement "if destroyed, degraded, or otherwise rendered unavailable, would" should be removed. There are enough criteria identified for High, Medium and Low BES impact without adding those elements that requires additional work not done today to answer. We are trying to increase reliability by having multiple cranking paths. But in doing so, it appears we are being penalized for identifying more cranking paths via these criteria. It seems sensible that robustness and redundancy should weigh into the criticality of an asset and this should be included this in this criterion.
HQT	Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. • The detailed Attachment 1 definition does give clarification. In any system where the Contingency Reserve is less than 2000 MW, clause 1.2 dominates clause 1.1 so engineering evaluation cannot be used to reclassify a Generation Subsystem into having a Medium BES Impact. Just because a Generation Subsystem is classified as Reliability "must run" doesn't mean the system can't survive if it fails (has a forced outage). Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. Request clarification on the wording "leaving" in 1.5. Also, 1.5 should be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station… Request clarification where 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include distribution

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	necessary to complete the cranking path? Why are blackstart related systems "High BES Impact"? The electric system has already failed when the "blackstart related systems" are needed. 1.10, 1.11 and 1.12 should be removed and language added to 1.7 as follows: Each Transmission Subsystem that, if destroyed, degraded or otherwise rendered unavailable, would result in exceeding one or more Interconnection Reliability Operating Limits (IROLs)or SOLs for those areas that do not identify IROLs, or exceeding limits requiring transmission loading relief (TLR), as determined by an engineering evaluation or other assessment method. Request clarification on 1.13, which SPS 300 kV threshold (550 kV for the Quebec Interconnection), sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. Also, 1.13 should be made to read: Each Protection System, Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have an Adverse Reliability Impact. Request clarification on "automatic load shedding" in 1.14. If this refers to under-frequency load shedding then Distribution Provider must be added to the Applicability Section. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center" Request clarification on wording "leaving" in 2.2. Also, 2.2 should be made to read: Each Transmission Subsystem that contains switching stations operated at 200 kV or higher in the Eastern and Western Interconnections, 300 kV or higher for Quebec Interconnection or 100 kV or higher in other Interconnections, not already included in section 1 above, with 3 or more transmission lines leaving the station… Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add ", including as notified by the Generation Owner" Consistent with 1.9, recommend changing 2.4 from "NUC-001-1" to "NUC-001" Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. Also, 2.5 should read: Each Protection System, Special Protection System (SPS) or Remedial Action Scheme (RAS) Subsystem operated at less than 300 kV in the Eastern and Western Interconnections, less than 550 kV for the Quebec Interconnection or less than 200 kV in other Interconnections that have an Adverse Reliability Impact. Consistent with the comment on 1.15 and 1.16, recommend changing from "Control Center and backup Control Centers" to "Primary Control Center and any backup Control Centers" in 2.6. Attachment 1 does not belong in a CIP document. Once implemented these definitions are likely to receive broad application.
Allegheny Energy	- Resolve the confusion of terms used in the proposed glossary additions.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	- Item 1.1 - What is the rational for 2,000 MVA value? (Why not 2,500 for example.) What would an example of an approved engineering evaluation be? - Item 1.2 addresses Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligation. It is not clear if this refers to the ISO/RTO obligation or to the entities' obligation. - Item 1.13 - "Adverse Reliability Impact" and other locations should be changed to "Adverse BES Reliability Impact." - There seems to be inconsistency in the use of MW vs. MVA
KCPL	The criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to "plug into" this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
Connectiv Energy	High, Medium and Low categories are adding a potentially unnecessary level of complexity. Transmissions Operators (TOPs) such as PJM which are concerned with and track such things as "contingency reserve", "reliability must run" status, "Nuclear", "voltage support" requirements, resulting "interconnect reliability operating limits" upon loss of a unit, and "black start" designations for the units in its system. As these are important to PJM for the operation of its grid, we as Generator Owners (GOs) and Generator Operators (GOPs) have used these as guides in determining which of our units are critical and would prefer not to have the FERC directly impose different requirements, but to work with the TOPs to reasonably influence criteria to be used in determining critical status.
MidAmerican	Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, MidAmerican recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) in question 13, but moving the categorization aspects of CIP-002-4 into the development work with security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. To demonstrate, see the following examples. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might be on the list as one, but not the only, acceptable method to achieve the objective of low electronic

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161 kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. If the security controls developed support the need for categorizations based on concepts in Attachment 1, the attachment should strive to eliminate the need for creating new definitions and concepts for these subsystems. Attachment 1 is hindered by the issues identified with the confusing definitions for Generation Subsystem and Transmission subsystem. Where meaningful categorizations are identified, their criteria should be bright line. MidAmerican recommends bright lines that do not necessitate engineering analyses or third party review. Bright line examples for substations would be substations with highest voltage connected at: 100-199kV are categorized as low, 200-299kV are medium and at or above 300kV are high. Substations connected at with highest voltage under 100kV are only in scope if they are part of the primary black start path. Bright line examples for generating units are units: rated at 100-299MW are categorized as low, 300-499MW are medium and at or above 500MW are high, as long as the unit is connected to the system at 100kV or above. Generating units under 100MW and/or connected to the system at under 100kV are only in CIP scope if the unit is a primary black start unit. Wind farm generating units are not in scope where the reliability of the BES is not designed to be dependent on the wind blowing.
CPG	For Item 1.2, what does the term "aggregate output" mean? Is that forcing GO/GOPs to evaluate their plants on an aggregate basis, even though they are separate Subsystems? For clarification, the wording should state "the MW or MVA output of the Generation Subsystem" so not to confuse the aggregate output of a plant with the aggregate output of the Generation Subsystem. For Item 1.5, who is the Reliability Assurer? For Item 1.5, it is common for a GO/GOP to communicate the impact levels of their assets to their interconnected TO/TOP, and vice versa. This is an excellent means to ensure the reliable operation of the Bulk Electric System.
Santee Cooper	Suggestions for improving proposed criteria: Simplifying the list. It seems to inter-mingled with Attachment 2. SC believes in the approach of determining which assets are critical to the reliable operation of the BES first, then assigning impact levels. For example, Blackstart units may not end up on the high impact list because of multiple cranking paths.
OGE	• 1.1 – if the Subsystem is "not essential to the reliability of the BES", why do these systems retain the overhead associated with the Medium BES Impact? This is essentially saying "all Gen Subsystems with aggregate name-plate generation >= 2,000 MVA

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	will be "High BES impact", unless you prove they are not essential… then you can drop them down to "Medium BES Impact". • In 1.1, "aggregate rated name-plate" is used and in 1.2 "aggregate output" is used. For consistency, should both state "aggregate rated name-plate". If not, 1.2 should state net output if that is the intent. • 1.4 – Needs to more specifically indicate "designated Blackstart Resource" per the regional blackstart capability plan. It should be noted that non-designated units may be referenced in the plan which could be construed as "included in the plan" {Reference EOP-005-2 R1.4} • 1.5 – Is it a subsystem that "contains" switching stations or are the switching stations themselves a Transmission Subsystem? • 1.5 - Lines "leaving the station" gets into direction of power flow. It appears the intent is lines "terminate (or intersect) at the station". • 1.5 – No indication that "…in which case…" these can be dropped to "Medium BES Impact" like 1.1, yet in 2.2, it indicates "not already included in section 1 above…" • 1.6 – Not clear what is intended by "Cranking Path". Should this be "Blackstart Cranking Path as designated in the regional blackstart capability plan or regional blackstart restoration plan? • 1.6 – Need to designate additional criteria, such as a threshold or the "primary" or "initial" cranking path, to include Transmission Subsystems in the "cranking path". In some cases several alternate cranking paths may be provided and it is counterproductive to include all alternate paths. • 1.10, 1.11 - Reference other standards that define the criteria / voltage collapse (TPL standards). • 1.12 - Use "BES" in place of "transmission system"? Wording makes criteria difficult to follow. Should "Adverse Reliability Impact" be used in place of "… or separation of Cascading outages."? • 1.12 - Is the intent for this to be "as determined through an engineering evaluation or other assessment method"? Should indicate an "approved" method for consistency? • 1.16 – Is the intent of the statement "… functions for transmission assets or generation assets of 2,000 MW or more." It is not clear in terms of transmission assets. First, this seems to deviate from the "MVA" ratings used earlier. Second, the phrasing no longer uses terms used earlier in the document such as "Transmission Subsystem" or "Elements". If the statement is specifying any transmission asset, it should state that (e.g. "… functions for any transmission assets…". If it is specifying transmission assets of 2,000 MW or more, it is not a clear method to describe transmission assets. • 2.5 – This category appears to be incomplete. Should this include the same statement as 1.13; "…that, if destroyed, degraded or otherwise rendered unavailable, …" ?
Oncor	Item 1.9, we propose to change "essential" to "required". Item 1.10, we propose to replace "in voltage collapse" with "in voltage collapse that would pose an unacceptable risk to the Adequate

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Level of Reliability of the BES". Item 1.12, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 1.13, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 1.16, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided. Item 2.4, we propose to change "essential" to "required". Item 2.5, we propose to add "as determined through an engineering evaluation or other assessment method" to the end of this statement. Item 2.6, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
PPL Supply	See response to #4 above.
St. George	As a small municipality, we applaud the draft team for dealing with the over-simplistic classification of an asset as Critical or Non-Critical. The proposed standard takes two classifications (Critical and Non-Critical) and makes three (High, Medium, and Low). We are deeply concerned that three classifications are not sufficient to represent the true nature of the BES. At minimum another classification should be added: Minimal. This would be for Generation Subsystems below 200 MVA and transmission below 150 kV in the Eastern and Western Interconnections. Low would then be for Generation Subsystems of 200 – 1,000 MVA and transmission of 150 – 200 kV in the Eastern and Western Interconnections. The Minimal classification assets would then be exempt from CIP-003 through CIP-009 in the same way Non-Critical assets are currently.
NGRID	• Suggestions for improving proposed criteria: • Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. • To distinguish between "must run" and "Reliability must run", recommend that 1.3 change from "must run" to "Reliability must run" • Request clarification on "leaving" in 1.5 • Request clarification are 1.4 and 1.6 refer to the primary restoration path or all restoration paths. Is it meant to include distribution necessary to complete the cranking path? • Recommend removing 1.10, 1.11 and 1.12 since none have an explicit threshold and is redundant with 1.7 plus does not provide enough details on who does these engineering studies or how they conduct such studies As per the discussion, it was noted that the redundancy of 1.10, 1.11, and 1.12 is because some areas do not have IROLs. In such a scenario, following is recommended

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	If 1.10, 1.11 and 1.12 exist to plug gaps in IROLs, then they should be sub bullets of 1.7 and start with something like "For those areas that do not use IROLs …" If 1.10, 1.11 and 1.12 remain; they need to address our concerns about "explicit threshold" and "who/how on the engineering studies" - Alternatively, number 1.13 (Protection System, SPS and RAS) needs to be deleted because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) • Request clarification on "automatic load shedding" in 1.14? If this refers to under-frequency load shedding then it may include distribution. • Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center" • Request clarification on "leaving" in 2.2 • Request a modification of 2.3 to make it consistent with 1.8 – at the end of 2.3 add ", including as notified by the Generation Owner" • Consistent with 1.9, recommend changing 2.4 from "NUC-001-1" to "NUC-001" • Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both? An SPS has a sensing portion and a portion that takes action and sometimes these are not the same voltage, same station, etc. • Consistent with the comment on 1.15 and 1.16, recommend changing from "Control Center and backup Control Centers" to "Primary Control Center and any backup Control Centers"
MGE	MGE does not support the three level approach. MGE would support a four level approach that has the addition of a "No BES Impact" category. This category would contain such cyber assets as contained in a Registered Entity's UFLS program or assets that don't currently impact the BES. The purpose of the UFLS program is to provide a last resort for system preservation. It is not defined in the UFLS Standards that the UFLS program is to maintain BES stability, but that is why there is a UFLS program. By not having a No BES Impact category, the SDT is not giving a bright-line solution for those entities who are only DP's with UFLS programs, etc.
FE	In general we disagree with the H/M/L classification driven by Attachment 1, and in particular some of the classifications between H/M seem arbitrary, especially the size of generation subsystems. We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. As presented, we believe Attachment 1 could be improved by eliminating 1.10, 1.11 and 1.12 which are redundant with 1.7.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
TECO	We support EEI's comments regarding attachment 1.
Snohomish	We have a concern with the MW thresholds that are used and that they do not actually identify impact risk. We prefer a more performance-based approach for both loss of load and generation, such as a utility or region cannot adversely impact neighboring systems.
CECD	2000/1000 MW or greater. - Nameplate rating should not be used to determine impact categorization, but rather actual tested capacity should be applied so that the real risk to the interconnection is examined. Furthermore, guidance indicates that a Generation Substation can be divided up into its components so it is not clear whether this will be interpreted the same way. Specifically, the guidance document states "The definition of a BES Subsystem is intentionally flexible to allow entities to evaluate their own particular power system design. For example a multiple unit generation facility can be defined as one or more Generation Subsystems depending on the functions being performed and the operational and technical characteristics of the generating unit." It is not proper to include frequency support as a factor for consideration in determining whether a unit is essential to the reliability of the BES. It is not clear how frequency support would be determined? For example, the loss of a 500 MW in the WECC footprint will have a much greater impact to frequency than the loss of the same unit in the Eastern Interconnection. In the Units larger than the Reserve Obligation criteria, is aggregate output referring to actual tested capacity? It is not appropriate to include a control center in the BES Subsystem category. A control center is more appropriately considered a Cyber System to be evaluated in relation to a BES Generation or Transmission Subsystem. Furthermore, language relating to control centers in Attachment 1 should use the term BES Transmission Subsystem and BES Generation Subsystem. It should also be clear whether the ratings apply to individual subsystems or all BAA subsystems in aggregate. There is a delicate balance between regulation supporting reliability measure and creating disincentives that may, in practice, reduce reliability. These standards must thoroughly consider the implications of imposing requirements to achieve reliability improvements not to hinder current reliability practices
MRO	We feel Attachment item 1.2 should include "for the Contingency Reserve Sharing Group" at the end of the statement to make the intent less ambiguous. Under Attachment item 1.2, we also feel the term "Reserve Sharing Obligations" should be defined in the NERC Glossary of Terms. Under Attachment item 1.3, we feel the term "Reliability must run units" should be defined in the NERC Glossary of Terms. Under item Attachment 1.4, we feel this represents the same "one size fits all" approach that the Guidance for the Electric Sector: Categorizing Cyber Systems document claims to be trying to eliminate. In reality, not all blackstart Generation Subsystems listed in the Regional Restoration Plan carry the same weight, or have the same impact on the region, so it seems like a hierarchy should be developed within the standard for categorizing these units as either High BES Impact, Medium BES Impact, or Low BES Impact. We feel this hierarchy should be based on the size of the Generation Subsystem (similar to the delineation defined by CIP-002-4 Attachment 1, sections 1.1 and 2.1, but not at the same MVA levels), as well as the Generation Subsystem's impact on the Regional Restoration Plan, such as if it has a role in cranking support for a nuclear plant. Attachment Item 1.4 currently does not differentiate between a utility having numerous blackstart capable Generation Subsystems, where

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	failure of multiple blackstart Generation Subsystems would not compromise their entire blackstart plan, or a utility with a single blackstart Generation Subsystem that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple blackstart Generation Subsystems, which makes their blackstart plan inherently more reliable. Under Attachment item 1.5, to remove ambiguity we feel we should replace “switching stations” with “switching stations or substations”. Attachment Item 1.6 currently does not differentiate between a utility having numerous Cranking Path options, or a utility with a single Cranking Path that is then essential to the success of their blackstart procedure. It seems a utility should be given consideration for having multiple Cranking Path options, which makes their blackstart plan inherently more reliable. Under Attachment item 1.9, the lack of a definition for “essential” makes this statement ambiguous. Under Attachment item 1.10, we propose to replace “in voltage collapse” with “in voltage collapse that would pose an unacceptable risk to the Adequate Level of Reliability of the BES”. Under Attachment item 1.12, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement. Under Attachment item 1.13, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement. Under Attachment item 1.16, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided. Under Attachment item 2.2, to remove ambiguity we feel we should replace “switching stations” with “switching stations or substations”. Under Attachment item 2.4, the lack of a definition for “essential” makes this statement ambiguous. Under Attachment item 2.5, we propose to add “as determined through an engineering evaluation or other assessment method” to the end of this statement. Under Attachment item 2.6, we do not feel transmission assets and generation assets should be judged against the same threshold, and a different threshold and clarification for quantifying transmission assets should be provided.
GTC	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
Xcel	We would like to see a category of ‘no impact’ for systems with no outside connectivity.
BGE	Consider the establishment of a reliability-based “Bright-line” methodology to remove ambiguity and assure the standard is applied consistently throughout the industry. Also, an alternative proposal to Attachment 1 is given in our response to Item #3.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
FPL	Suggestions for improving proposed criteria: Regarding High BES Impact 1.1, we believe approving assessment methods should be the function of the Regional Entity and/or NERC and the roles of the RC will need to be explicitly defined. In cases where the RC function has been delegated to a utility agent, we feel controls should be in place to avoid conflict of interest and/or shield the agent from liability. Regarding High BES Impact 1.2, we suggest striking this criterion. Independent Generators do not have access to the information described in 1.2 and therefore cannot assess their Generator Subsystems appropriately. We also suggest striking the term “Adverse Reliability Impact” as it is not defined in the Glossary of Terms. We also suggest amending the standard to filter only for those Generators that are “primary blackstart.” Many generators may be included in a restoration plan, but are of secondary or tertiary value and not all blackstart units are equal.
TAPS	See TAPS response to Question 1.i.
Allegheny power	AP is in agreement with EEI’s amended Attachment 1.
FMPA	High BES Impact (H): FMPA recommends that criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region). The EPAct, FPA Section 215(a)(4) defines “reliable operations” as: “operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such systems will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements," so, to boil it down, the EPAct passed into law mandatory standards to regulate the industry in its efforts to avoid "instability, uncontrolled separation, or cascading failures" This definition of "reliable operation" is nearly synonymous with the NERC Glossary term for "Adverse Reliability Impact": "(t)he impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." "Cascading" is further defined by the NERC Glossary as: "The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies." The focus of the standard ought to use this concept of Adverse Reliability Impact to define what is High risk, Medium risk and Low risk. Supply/Demand Mismatch and IROL: Starting from this theoretical basis, what kinds of conditions can cause an Adverse Reliability Impact, such as widespread frequency related instability? The answer really is a large mismatch of supply and demand (even faults can cause instability by "shorting out" the load, causing a large mismatch of supply and demand) or operating conditions, regardless of cause, that lead to violation of an Interconnection Reliability Operating Limit (IROL). Therefore, the entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs. The rest of Attachment 1 is simply a restatement of conditions that can cause these metrics to be exceeded. IROL is defined in the NERC glossary as: "(a) System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System." IROLs are determined by study by the PAs and

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	TOPs and these metrics are readily available in accordance with FAC-014. Hence, the only metric that remains to be established is the supply/demand mismatch. This mismatch can be caused in a few ways: 1. Tripping a large amount of generation through malicious use of cyber systems 2. Tripping a large amount of load due to malicious use of cyber systems to directly trip the load (e.g., use of a large SCADA system to activate a centralized UFLS system). 3. Tripping key transmission Facilities by malicious use of cyber systems that could cause voltage instability, thermal cascading, etc., that could in turn result in a large mismatch of supply and demand, the large mismatch of supply and demand being the key. (For example, the Northeast Blackout of 1965 was caused by loss of tie lines importing power from Canada causing a large supply/demand mismatch, and the Blackout of 2003 was caused first by thermal cascading, which in turn caused a voltage collapse of Cleveland and Detroit, which then resulted in a huge supply /demand imbalance through the loss of two major urban centers) FMPA recommends that the SDT develop a metric for supply/demand mismatch (e.g., the Contingency Reserves of the region, or another metric determined by study) that correlate with High and Medium Impact. High Impact should include those events that have a relatively high chance of causing an Adverse Reliability Impact, e.g., cause an IROL to be exceeded or a supply / demand mismatch greater than a certain metric. Finally, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold and 1000 MVA/1000 MW for the Medium BES Impact threshold. 2000 MVA may be an acceptable default value for High Impact in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for the region. 1000 MVA may be an acceptable default value for Medium Impact in the absence of a specific regional threshold based on the largest single contingency for a PC or RC. Blackstart and Cranking Paths: If a wide-spread outage were to occur, utilities need to be assured that their blackstart units and cranking paths to other generators that are identified in the regional restoration plan will be available, and that the control systems for these devices have not been compromised. FMPA understands the need for protection of the “critical units” and “critical paths,” but the identification of all blackstart units as High Impact is not reasonable or necessary to ensure BES restoration. FMPA recommends that the categorization of blackstart units and transmission cranking paths between the blackstart units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, “High Impact” from a restoration perspective should focus on preventing restoration efforts and “Medium Impact” should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent blackstart efforts from multiple blackstart units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder blackstart efforts from a single blackstart unit or cranking path in the regional plan. Blackstart capable units that are not in the regional plan should be Low Impact. Recommendation of Edited Language to High BES Impact: 1. High BES Impact (H)

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	1.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the Contingency Reserve or total Reserve Sharing Obligations of a Reserve Sharing Group or, if no Contingency Reserve or total Reserve Sharing Obligation has been established, a supply loss of 2000 MVA or a load loss of 2000 MW. 1.2. Each Control Center and backup Control Center performing Reliability Coordinator functions. 1.3. A BES Cyber System, that if maliciously used, can result in exceeding one or more Interconnection Reliability Operating Limits (IROL's). 1.4. A BES Cyber System, that if maliciously used, can prevent blackstart restoration efforts from multiple black start units and cranking paths identified in the regional restoration plan. FMPA believes using the above criteria would make Attachment 1 very simple, resulting in only four criteria instead of the 16 in the "High Impact" list proposed by the SDT. Most of the 16 items in the "High Impact" list are simply phenomena that can cause supply/demand mismatch greater than the established metric, or an IROL to be exceeded (e.g., voltage collapse, thermal cascading, loss of situational awareness, etc.) We recommend including these phenomena as subsections of the four criteria spelled out above. We believe such a method is much simpler to understand and enforce, and is more in line with what ought to be regulated - phenomena that can cause an Adverse Reliability Impact. If the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 2000 MVA/2000 MW for the High BES Impact threshold. 2000 MVA may be an acceptable default value in the absence of a specific regional threshold based on Contingency Reserve or total Reserve Sharing Obligations for a PC or RC. Recommendation of Edited Language to Medium BES Impact: Medium Risk should be those events that would put the system dangerously close to an additional contingency causing an Adverse Reliability Impact, e.g., an event that could cause a supply / demand mismatch greater than the largest loss of source that would put the system in a status whereby a single contingency could cause a supply / demand mismatch greater than the Contingency Reserves of a reserve sharing group, or an IROL to be exceeded, (at a point only a single contingency away). Also, if the bright line impact thresholds are kept, the SDT must provide a technical rationale for selecting 1000 MVA/1000 MW for the Medium BES Impact threshold. 1000 MVA may be an acceptable default value for the Medium BES Impact threshold in the absence of a specific regional threshold based on the largest single source contingency. 2. Medium BES Impact (M) 2.1. A BES Cyber System, that if maliciously used, can cause a supply/demand mismatch greater than the single largest loss of source contingency of the region, or, if no single largest loss of source value has been established, a supply loss of 1000 MVA or a load loss of 1000 MW. 2.2. A BES Cyber System, that if maliciously used, can result in a system state whereby the next single contingency would cause the BES to exceed an IROL. 2.3. A BES Cyber System, that if maliciously used, can hinder regional blackstart restoration efforts by preventing blackstart from a single black start unit and cranking path identified in the regional restoration plan.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Low BES Impact (L): Low Impact should include all other BES systems that have a low risk of contributing to an Adverse Reliability Impact. FMPA cautions the SDT that even though the Low BES Impact category will have the least impact to reliability, it will have the most burdensome and widespread impact on registered entities for compliance purposes. We cannot stress this point enough; the industry needs assurance that the Low BES Impact requirements will be reasonable, and preferably, no requirements since it would seem beyond the scope of the FPA. If there are any requirements in CIP-003 and higher for Low Impact cyber systems, those requirements must be aligned with the cyber system protections that are programmatic in nature and are not cyber system specific. These requirements should be similar to the current CIP-002, which require a risk based assessment methodology where entities can manage compliance through employee training on the security of cyber assets, etc. Making the compliance requirements exceedingly strict will take valuable resources away from the protection of the high and medium impact assets. The industry's first priority should be to protect and secure the high and medium impact facilities.
Duke	Attachment 1 is not needed for the "Cyber First" approach. Any Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact, and protected accordingly.
NBSO	Considerations for improving proposed criteria: 1.1: Simply use a threshold number of 2000 MVA. Do not have the RC/RA held responsible to omit a generator. Alternatively I would see that the RC may overrule and provide a lower value threshold if necessary. 1.2: The "largest value of Contingency reserve" is not clear. Using a dynamic number in 1.2 is inconsistent with CIP implementation that needs a long lead time. By comparison 1.1's threshold is consistent. Suggest using a percentage of largest contingency to protect against those times were the typical largest contingency is reduced. 1.3: Recommend that 1.3 be removed because must run unit commitments can vary real time depending on system configurations. A system must be planned and operated considering the loss of the must run unit regardless if a cyber incident or equipment malfunction. There appears to be overlap in 1.5, 1.8, 1.10, 1.11, 1.12 There should be some attempt to be more crisp, focusing on eliminating those situations where there is a increased risk to the bulk system due to the risk of exceeding credible contingency assumptions. Some of these are part of these items are in the SOL definition, so why not use SOL? 1.13: Needs clarity. Should consider all SPS's that would impact the BES. These could operate at a lower voltage then those listed. 1.14: For smaller areas the 300 MW threshold may be too large. Consider allowing RC input to lower this value. 1.16: "Transmission assets of 2000 MW or more" should be better defined. "Generation assets of 2000 MW or more" should also be better defined. Is it total generation capacity greater than 2000 MW. Since some Control Centers do not have a backup, recommend changing 1.15 and 1.16 from "Each Control Center and backup Control Center" to "Each primary Control Center and any backup Control Center"

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	In addition - there is no consideration for generation with a common control system or cyber asset that may span two or more RC foot prints. - there is no consideration for a common cyber system that may control large loads. As well as how the acceptable loss of load threshold for a given area is determined. Could this be an RC responsibility to determine the maximum acceptable load loss? Also the DP should also be considered in the applicability section.
AESI	The ability to evade the bright line criteria through the use of an engineering study will lead to inconsistent application of the standards. As written, the Low BES Impact category would contain widely disparate subsystems. There should be a specific list of criteria for Low BES Impact that includes some BES Subsystems, but not all that do not qualify as High BES Impact or Medium BES Impact.
IESO	5. Although Adequate Level of Reliability #5 (ability to restore the system) is included as a critical function, it is limited to blackstart generation and transmission subsystem cranking paths. H and M criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). We would drop 6 generating stations (over 3000 MW) from High (current Critical Assets) to Low using the proposed categorization criteria. There should be a requirement in the High category for generation essential to facilitate restoration as determined by the RC. Item High 1.7 - Exceeding an IROL does not cause instability if recovered within the timeframe allowed by the current standards requirements, and therefore should not be a H or M criterion TLRs are more often used to manage constraints that are binding due to market-market activity. TLRs in and of themselves do not necessarily affect reliability, therefore should not be H or M criteria
Manitoba 2	All comments are prefaced with the section number: 1.3 - Must Run units may only be needed for local area congestion management and therefore should have a Medium BES Impact. All of the High BES Impacts should be prefaced by the question - Do they contribute to instability, separation or cascading? 1.4 - A blackstart plant is not typically critical because there are alternatives available in most blackstart plans. Blackstart plants should be in the Medium BES Impact category unless their size includes them in section 1.1 or 1.2. 1.5 - A 300 kV or higher substation may or may not be critical. If the station loss lead to instability, separation or cascading, then it has a High BES Impact, which is already addresses in sections 1.10 to 1.12. 1.6 - There are typically alternative Cranking Paths. Transmission Subsystems comprising the Cranking Paths should be a Medium BES Impact. 1.13 – These systems shouldn't have an Adverse Reliability Impact. This criteria should instead refer to instability, separation or cascading. 2.2 – This criterion should be qualified as having an Adverse Reliability Impact. 2.5 – A lower bound is required for this criterion, and should be revised to “Each Protection System, Special Protection System, or Remedial Action Scheme Subsystem operated at less than 300 kV and at 100 kV or more in the Eastern and Western Interconnections,

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	or less than 200 kV and at 100 kV or more in other Interconnections that have an Adverse Reliability Impact". 2.6 – "Not included above" should be revised to "not already included in Section 1 above." 3.0 - By the definition, these BES Subsystems do not have an impact on the reliability of the BES, and therefore should belong in a "No BES Impact" category. If a No BES Impact category is not provided, the controls for the Low BES Impact category should not be auditable.
ATC	Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (ATC Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entities are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit. 1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: ATC removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity.

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? As a Transmission only company ATC would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or generation) ATC believes strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.) Additional comments on the SDT Attachment 1 document: 1.7 A TLR is a tool used by entities to help control system limits in both a pre-contingency or post-contingency event. We disagree with the SDT assumption that an IROL is equal to a TLR event and therefore should both be identified as high. We recommend that this language be removed from Appendix 1. (NOTE: TLR's are only issued in the Eastern Interconnection.) 1.10 - .12 ATC believes that these should be deleted because they do not fall into the goal of Attachment 1. The goal of Attachment 1 is to provide greater clarity around what BES Facilities should be categorized as either High or Medium. The way these items are written it would force all registered entities to study all of its Transmission Subsystem and show that they do not cause cascading, instability or separation. The other options for the SDT (one we don't recommend) would be to delete items 1.1 – 1.9 because 1.10 and 1.12 requires

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	us to perform engineering assessments.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
IMPA	In 1.12., 2.3, it does not state how an entity is to come to the conclusion of a complete operational failure or cascading outages. It should say as determined through an engineering analysis or other assessment method. In 1.13, 2.5, it does not state how an entity is to come to the conclusion of an item having an Adverse Reliability Impact. IMPA recommends adding as determined through an engineering analysis or other assessment. IMPA would like to see the addition of an impact category for BES Subsystems that have an extremely minimal impact on the BES, and do not get assigned a high percent (70 or 80 percent) of the security requirements for a High or Medium BES Impact asset.
ERCOT	ERCOT ISO supports Midwest ISO Comments. To further improve the proposed criteria, ERCOT ISO recommends that the criteria be based on time frame as well as impact to the BES. Midwest ISO Comments: 1. Suggestions for improving proposed criteria: What is the basis for these criteria? Without any basis, we have to assume that many of the criteria are arbitrary. For example, what is the basis for the 2000 MVA and 1000 MVA generation numbers in the High and Medium BES Impact categories? 2. In Item 1.3 revise the reference to a "Must Run" unit to add the following phrase at the end of the sentence: "...that have wide area reliability impacts." 3. Add an Item in Category 2 that corresponds to Item 1.3 for "Must run" units that have "local area reliability impacts." 4. In Item 2.6., the word "controlling" needs to be clarified. This item should only encompass Control Centers and back up Control Centers that "remotely control and solely monitor the status of assets" rather than just performing redundant monitoring of those assets. ISO-NE Comments: The Standard should not reference the role of a Reliability Coordinator or Reliability Assurer reviewing a Responsible Entity's "engineering evaluation or other assessment method ". 1. Requirement 1.2 anticipates a so-called "Reliability Assurer" as playing a role in the determination of which BES Subsystems contain Cyber Systems that may be subject to required cyber-security/critical infrastructure protections. 2. If the SDT, in fact, intended for a Reliability Coordinator or Reliability Assurer to have an obligation to review and ultimately approve Responsible Entity's evaluations/methods, such a Requirement would be contrary to Order Nos. 706 & 706-A. By including in a Reliability Standard that a Reliability Coordinator may approve evaluations/methods, the Standard Drafting Team appears to place ultimate responsibility on the designation of assets as requiring critical infrastructure protections on the Reliability Coordinator. Order No. 706A reaffirmed that a Responsible Entity must be solely responsible for identifying those assets that are subject to critical infrastructure protections. In Paragraph 53 of 706-A, FERC stated that: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
PacifiCorp	Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. PacifiCorp submits that the security controls work must be completed to determine what categorizations are possible and needed. PacifiCorp has reviewed the existing controls and observes the following: many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, PacifiCorp recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) in question 13, but moving the categorization aspects of CIP-002-4 into the development work with security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might on the list as one, but not the only, acceptable method to achieve the objective of low electronic authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, PacifiCorp submits that the development of Attachment 1's concepts be concurrent with the security controls work. If the security controls developed support the need for categorizations based on concepts in Attachment 1, the attachment should strive to eliminate the need for creating new definitions and concepts for these subsystems. Attachment 1 is hindered by the issues identified with the confusing definitions for Generation Subsystem and Transmission subsystem. Where meaningful categorizations are identified, their criteria should be bright line. PacifiCorp recommends bright lines that do not necessitate engineering analyses or third party review. A bright line approach will ensure consistent, standardized, and auditable requirements. Further, a bright line approach, if designed properly, will be an effective and efficient way to protect the BES from a concerted well-planned cyber attack. Specifically, PacifiCorp suggests the following to improve the specific criteria currently listed in Attachment 1: • Section 1.4, 1.6: PacifiCorp suggests that the Cranking Path requirement be further defined. Many utilities have designated many

Organization	Question 8 Suggestions for improving proposed criteria (Response page 20)
	potential cranking paths, some which are considered primary or preferred paths while others are alternative paths. PacifiCorp suggests establishing a megawatt level criteria in order to properly categorize the impact to the BES of different blackstart units and Cranking Paths. For instance, small generating units under a certain megawatt nameplate could be excluded unless the unit is in the primary black start path because the other small units have minimal risk of contributing to success of a concerted, well-planned attack against multiple points. • Section 1.5: PacifiCorp suggests that the specific number of lines coming from a substation should not be a consideration. Rather, the specific nature of the lines i.e. station duty, fault duty and flow levels, should be considered. • Section 1.13: The reference to SPS or RAS Subsystem is unclear. PacifiCorp would currently consider its SPS to be a cyber system, housed within a critical substation. PacifiCorp suggests that SPS Subsystem should be defined separately.
PEPCO	Proposed amendments to Attachment 1 were provided earlier.
NEI	A) Suggest rewording 1.2 to strike reference to contingency reserve or total reserve sharing obligations. The wording is suggested to be "Any critical generating unit or plant." B) The functional approach for determining impact categories would provide the opportunity to clearly define what is most important and what needs the greatest attention. It's important to recognize that most any system is designed to continue to operate successfully, even under conditions where some parts are not optimally functioning. The factor of how long can you continue with without certain components helps to prioritize the protection necessary. Also, many systems contain algorithms to address fault conditions and back-up components for failed occurrences. These factors don't seem to come into consideration under the current draft standard approach. C) Apply them appropriately. Hierarchical categorization of loss impact of individual electric operating sites/assets may be useful in defining physical security standards. But electric grid asset rating/size categorization is not salient to definition of hierarchical security controls and countermeasures requirements for cyber assets. Hierarchical sets of requirements (controls and countermeasures) are needed for cyber assets themselves, based upon how much risk they themselves pose to reliable operation of the bulk electric system should they be lost or compromised. D) In general we disagree with the H/M/L classification driven by Attachment 1, and in particular some of the classifications between H/M seem arbitrary, especially the size of generation subsystems. We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use. E) As presented, we believe Attachment 1 could be improved by eliminating 1.10, 1.11 and 1.12 which are redundant with 1.7.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

Summary Consideration for LSEs: The vast majority of respondents had no suggested criteria for LSEs (or the other proposed functional entities). In fact, most felt that these entities should not be included as responsible entities in this standard. Those that felt that they should be included added that it depended on whether they had BES Cyber Systems. Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)

Organization	Question 9 Comments for LSE (Response page 21)
GSOC/OPC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Consumers	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
MPPA	MPPA has concern expanding the applicability to Load-Serving Entities. Any BES assets a LSE may have should be sufficiently covered by the attachments. Adding LSE's does not add value or increase the reliability of the BES.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since LSEs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Calpine	Suggested Criteria for load serving entities

Organization	Question 9 Comments for LSE (Response page 21)
	Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
Flathead	Eliminate Low BES Impact assets as by definition they are not critical.
Carthage	Can this function impact the BES in real time? If so, please explain how. Should this function automatically be placed in the Low BES Impact category? If not please explain why.
Entergy	Use of “routable protocols” is the bright line sought, regardless of electric asset size/rating/type. See Entergy’s response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Load Serving Entities: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	Load Serving Entities should have applicability to the standard only if they operate transmission protection equipment or Special Protection Systems (SPS)
O&R	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
Alliant	We believe they should not fall under the applicability of this Standard.
Ameren	From a System perspective, loss of load should be commensurate with the loss of generation. This would be applicable to LSE
Black Hills	Not at this time.
NVEnergy	None; these entities do not generally impact the reliable operation of the BES.

Organization	Question 9 Comments for LSE (Response page 21)
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	Given that a LSE that owns assets used to serve customer load is also a Distribution Provider, we do not see any reason to include the LSE function in the applicability of this standard (include the DP)
BPA Trans	none
KCPL	No comments
MidAmerican	The characteristics and connectivity of their Cyber Assets will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
CPG	No comment
Santee Cooper	no
Oncor	We question whether they should even fall under the applicability of this Standard.
NGRID	National Grid does not have any suggested criteria for LSE, TSP, or IC.
MGE	LSEs should be removed from the applicability section of this Standard.
FE	"Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS.
TECO	We support EEI's comments on this item.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
Allegheny power	AP proposes following the example of the amended Attachment 1, namely: • Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern

<table>
<tr><th>Organization</th><th>Question 9 Comments for LSE (Response page 21)</th></tr>
<tr><td></td><td>and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have a material adverse reliability impact,
• Subsystems that perform automatic load shedding of 300 MW or more.</td></tr>
<tr><td>FMPA</td><td>The same criteria should be used for all Entities because the bottom line is avoiding “instability, uncontrolled separation, and cascading”, which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.</td></tr>
<tr><td>Duke</td><td>Any LSE Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.</td></tr>
<tr><td>AESI</td><td>none</td></tr>
<tr><td>ATC</td><td>LSEs should be removed from the applicability section of this Standard. LSEs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems</td></tr>
<tr><td>LES</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Organization</th><th>Question 9 Comments for LSE (Response page 21)</th></tr>
<tr><td></td><td>
<table>
<tr><td>-Public</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.</td></tr>
<tr><td>IMPA</td><td>none</td></tr>
<tr><td>PacifiCorp</td><td>Suggested Criteria for Load Serving Entities: The standard should apply to Load-Serving Entities if they operate transmission protection equipment or a Special Protection System (SPS).</td></tr>
<tr><td>PEPCO</td><td>Load Serving Entities should have applicability to the standard only if they operate transmission protection equipment or Special Protection Systems (SPS)</td></tr>
</table>

Summary Consideration for TSPs: The vast majority of respondents had no suggested criteria for TSPs (or the other proposed functional entities). In fact, most felt that these entities should not be included as responsible entities in this standard. Those that felt that they should be included added that it depended on whether they had BES Cyber Systems. Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)

Organization	Question 9 Comments for TSP (Response page 21)
GSOC/OPC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since TSPs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Carthage	No comments
Entergy	Use of "routable protocols" is the bright line sought, regardless of electric asset size/rating/type. See Entergy's response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Transmission Service Providers: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	TPSs should be removed from the applicability section of this Standard. TPSs do not own or operate BES Subsystems or have the

Organization	Question 9 Comments for TSP (Response page 21)
	means to evaluate the impact of BES Cyber Systems.
Alliant	We believe they should not fall under the applicability of this Standard.
Black Hills	Not at this time.
NVEnergy	None; the requirements applied to the Transmission Owner/Operator are sufficient.
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	none
BPA Trans	none
KCPL	No comments
MidAmerican	TSPs do not have cyber assets.
CPG	No comment
Santee Cooper	no
Oncor	We question whether they should even fall under the applicability of this Standard.
MGE	TSPs should be removed from the applicability section of this Standard.
FE	TSP facilities interact with the BES like a control center. Therefore, TSP Cyber Systems should be categorized as like a Control Center.
TECO	We support EEI's comments on this item. However, we note that EEI may have used the acronym TPS instead of TSP.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.

Organization	Question 9 Comments for TSP (Response page 21)
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any TSP Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.
AESI	none
ATC	TPSs should be removed from the applicability section of this Standard. TPSs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems.
PSE	It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.
IMPA	none
PacifiCorp	Suggested Criteria for Transmission Service Providers: The standard should not be applicable to Transmission Service Providers because Transmission Service Providers to not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type. • High = data/control/operations/system administration centers using TCP/IP networking; • Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.

Organization	Question 9 Comments for IC (Response page 21)
GSOC/OPC	none
APPA	In general LSEs, TSPs and ICs do not own and operate BES Facilities. To the extent that they own and operate BES Cyber Systems, they should be treated the same as other registered entities.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. Since ICs do not own the assets in question, they should be removed from the applicability section.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Carthage	No comments
Entergy	Use of "routable protocols" is the bright line sought, regardless of electric asset size/rating/type. See Entergy's response to Question 13 for further discussion.
CenterPoint	Suggested Criteria for Interchange Coordinators: None at this time.
NIPSCO	We do not have any suggested criteria for LSE, TSP or IC, but believe that if the SDT is unable to identify any specific criteria for the inclusion of these entity types for applicability then these three entities should be removed from the standard.
ConEd	The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
EEI	EEI proposes following the example of the amended Attachment 1, namely, only those entities that operate: • Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystem operated at 300 kV and above in the Eastern and Western Interconnections, or operated at 200 kV and above in other Interconnections, that, if destroyed, degraded or otherwise rendered unavailable, would have a material adverse reliability impact,

Organization	Question 9 Comments for IC (Response page 21)
	• Subsystems that perform automatic load shedding of 300 MW or more.
Alliant	We believe they should not fall under the applicability of this Standard.
Black Hills	Not at this time.
NVEnergy	No criteria are necessary; interchange coordinator does not have the capacity to affect the security of the BES.
Empire	This entity should not be included. Can they impact the BES in real time?
SCEG	none
Exelon	none
BPA Trans	none
KCPL	No comments
MidAmerican	This is not a defined entity in the NERC Glossary.
CPG	No comment
Santee Cooper	no
OGE	• Should these entities be included? • Can they impact the BES in real time? • Do they automatically go to Low BES Impact?
MGE	ICs should be removed from the applicability section of this Standard.
Teco	None
MRO	We feel they should not fall under the applicability of this Standard.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.

Organization	Question 9 Comments for IC (Response page 21)
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any Interchange Coordinator Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact.
AESI	None We believe that neither Load Serving Entities nor Transmission Service Providers should be covered by these standards.
ATC	ICs should be removed from the applicability section of this Standard. ICs do not own or operate BES Subsystems or have the means to evaluate the impact of BES Cyber Systems. Lastly, ATC does not have any suggested criteria for LSE, TSP or IC, but believes that if the SDT is unable to identify any specific criteria then these three entities should be removed from the standard.
PSE	It would be relative to actions as a result of a Reliability Directive that require Cyber Systems to implement.
IMPA	none
PacifiCorp	Suggested Criteria for Interchange Coordinators: Interchange Coordinator is not a term defined in the NERC Glossary. See response to question 8 for all three of the above. The characteristics and connectivity of their Cyber Assets will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type. • High = data/control/operations/system administration centers using TCP/IP networking; • Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.
NEI	Suggest dropping LSE and using DP in its place. However, it is recognized that: "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. Conceptually, recommended practically- salient cyber impact categories are listed below. These are the same regardless of Entity type. • High = data/control/operations/system administration centers using TCP/IP networking;

Organization	Question 9 Comments for IC (Response page 21)
	• Medium = field assets (substations, generation) using TCP/IP communications; and anywhere dial-up is used; • Low = everything else cyber that doesn't employ routable protocols. Use of "routable protocols" is the *bright line* sought, regardless of electric asset size/rating/type.

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

Summary Consideration: The only respondents that felt these entities should be included said that NERCNet was probably the only concern. Several felt that even NERCNet would not affect the BES.

Organization	Question 10 Comments (Response page 22)
GSOC/OPC	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
Consumers	Comment #1: We believe that NERC and Regional Entities should have to identify those Cyber Systems that contain industry sensitive information. (Examples: Associated with TFE requests or Sensitive National Security Information) Comment #2: We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
NPCC	Recommend that the SDT review the impact of NERCnet and Cyber Systems connected to NERCnet.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. These entities do not own the assets in question, so they should be removed from the applicability section. Unless of course the SDT takes our suggestion above under Q7. If so, all other registered entity types but NERC and the REs should be removed.
Dominion	No suggested criteria.
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: We believe that NERC and Regional Entities should have to identify those Cyber Systems that contain industry sensitive information. (Examples: Associated with TFE requests or Sensitive National Security Information) Comment #2: We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	No suggestions. If the entity has a cyber system that impact a critical BES function, the criteria should be the same for all entities regardless of their function.
SOCO	Unless there are no requirements at all for cyber systems associated with low-risk BES Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all low-risk subsystems should be exempt from the standard CIP-003 through CIP-009,

Organization	Question 10 Comments (Response page 22)
	or a category for minimal-risk or no-risk subsystems must be created.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Edison Mission	1. Although it is not known to us at this point what controls or levels of protection would be required for the 3 suggested levels of High, Medium or Low impact. I would like to suggest that there also be a fourth category of No Impact. It would seem to me that there are more than a few generating facilities that would have no impact on the reliability of the BES be it a small generating station or wind facility. 2. In CIP-002-4 under Attachment 1 under High Impact (1.4) it states that "Each Blackstart Generation Subsystem that has been included in the regional Blackstart capability plan" Some Blackstart units included in the Blackstart capability plan are not necessarily critical to restoration of the BES if there were a power outage.
Calpine	Suggested Criteria for load serving entities Impact categories should be based on generating capacity and generation time criteria. Define peaking unit vs. base load unit. Peak units would be those units operation <50% of mean operation time over 12 months. Base load units would be those units operation >50% of the time. Low impact Base unit with <300 MW Medium impact Base unit with <1000 MW High impact Base unit with <2000 MW Low impact Peak unit with <300 MW Medium impact Peak unit with <1000 MW High impact Peak unit with <2000 MW Black start plants required for grid restoration would be considered High impact.
Flathead	Eliminate low impact.
Carthage	No comments
Entergy	See Comments under Question 13; most likely “High”
CenterPoint	Suggested criteria for NERC and Regional Entities: None at this time. It is not clear criteria needs to be developed for these entities.
NIPSCO	We are concerned that due to the potential scope of the proposed CIP V4 modifications, that NERC and the Regions own and operate

Organization	Question 10 Comments (Response page 22)
	cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.. Suggestion: Review the intended scope of the term control center and clarify the intent with revised or additional language.
ConEd	The criteria should be simplified and having 3 levels makes determining which one applies very difficult and confusing.
EEI	NERC and the Regional Entities can voluntarily adopt these requirements if they believe that the requirements are necessary for their organization. NERC also has the option to require all or certain requirements to the Regional Entity through the Delegation Agreement.
O&R	Please refer to question 8. The Drafting Team should consider use of an impact-based methodology such as the NPCC A10 Criteria.
Alliant	We believe they should not fall under the applicability of this Standard.
Ameren	We see no role for NERC or Regional Entities in this regard as these entities should make sure that they have nothing that is capable of impacting the operation of the BES.
Black Hills	Not at this time.
NVEnergy	None; NERC and Regional Entities do not own or operate BES facilities, and therefore no criteria would apply.
MWDSC	Recommend creating a separate category for "No BES Impact". Criteria would be to demonstrate no Adverse Reliability Impact using an engineering evaluation.
Empire	These entities should be outside of the scope of this standard.
SCEG	If NERC/Regional Entities are considering collecting/retaining any information pertaining to CIP-002-4 from entities, any systems responsible for housing/managing/retaining such information should be considered a high impact category.
Exelon	No opinion at this time.
BPA Trans	Suggested criteria for NERC and Regional Entities: The criterion needs to be simple and clear. Criteria such and MW generation or load served by a transmission system is good. Criteria that requires studying loss of equipment beyond that done for normal planning creates additional workload with little benefit.
HQT	Recommend that the SDT review the impact of NERCnet and Cyber Systems connected to NERCnet
Allegheny Energy	We are concerned that due to the potential scope of the proposed CIP-002 version 4 modifications, that NERC and the Regions own and operate cyber systems that would become subject to these standards. Concerns exist in regards to the impact on those entities and the necessity for system modifications, communication path security, account management, availability, etc.
KCPL	No comments

Organization	Question 10 Comments (Response page 22)
MidAmerican	See response to question 8 and 9. The characteristics and connectivity of their Cyber Assets, if any, will drive which security controls are relevant. The relevant security controls and span of control of the Cyber Assets will drive meaningful categorizations of high, medium or low.
CPG	No comment
Santee Cooper	no
OGE	• Should these entities be included? • Can they impact the BES in real time? • Do they automatically go to Low BES Impact?
NGRID	It is not clear as to why the SDT is including NERC and Regional Entities in the applicability of this standard. NERC and Regional Entities are not subject to the Compliance and Enforcement Program and therefore having them list in the applicability section only confuses the issue of who has to comply with this standard.
MGE	They should be removed; neither has any impact on the real time reliability of the BES and are not users, owners or operators of the BES.
TECO	We support EEI's comments on this item.
MRO	We feel they should not fall under the applicability of this Standard.
GTC	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
Xcel	We feel they should not fall under the applicability of this Standard
BGE	There should be clearly defined, quantifiable criteria in order to apply the standard consistently among all entities.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	Any NERC or Regional Entity Cyber System that could be exploited to impact BES reliability should be categorized in terms of its risk and impact, and protected accordingly.
AESI	The standards should apply with respect to information related to BES Cyber Systems that is under their control.
ATC	ATC does not understand why the SDT is including NERC and Regional Entities in the applicability of this standard. NERC and Regional Entities are not subject to the Compliance and Enforcement Program and therefore having them list in the applicability section only

Organization	Question 10 Comments (Response page 22)
	confuses the issue of who has to comply with this standard. NERC and the Regional Entities can voluntarily adopt these requirements if they believe that the requirements are necessary for there organization. NERC also has the option to require all or certain requirements to the Regional Entity through the Delegation Agreement. We believe that these two entities should be deleted from the Applicability Section.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from

Organization	Question 10 Comments (Response page 22)
	implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
IMPA	none
ERCOT	The functions of NERC and the Regional Entities do not lend them to alignment with the CIP standards. However, the information they possess could have a severe, if indirect, long term impact on the BES if not properly protected. With this in mind, it may be necessary to draft additional guidance for NERC and the Regional Entities regarding information protection. This would provide adequate instruction to NERC and the Regional Entities as well as provide a level of understanding and assurance for other Responsible Entities.
NEI	A) Clarify that the purpose of the question is to differentiate between the criteria for LSE, TSP and IC and the criteria for NERC and ROs. B) If yes, then see #9 – no different; most likely "High"

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?

Summary Consideration for Distribution Provider: Results for the Distribution Provider (DP) were mixed. Some felt that the DP could be excluded, since they did not involve facilities >= 100kV. Some felt that the DP should be substituted for the LSE. Some were unsure how load shedding and Smart Grid would affect this standard. Some were very opposed, feeling this opened distribution up to FERC regulation. There are many criteria that can direct affect Distribution Providers, especially when considering the NERC registration criteria for Distribution Providers. Such attachment 1 criteria for Protection Systems and UFLS can directly affect DP's that have such systems that are relevant for BES reliability. Registration criteria also point out that DPs that also satisfy Load Serving Entity registration criteria should register as LSEs. The SDT has included DPs in the list of applicable Responsible Entities.

Organization	Question 11 Comments for DP (Response page 23)
Progress Energy	The DP should be added if it has cyber systems that could access and impact the reliability of the BES and/or if the DP owns cyber systems that are shared with Transmission subsystems.
GSOC/OPC	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Hayden	If NERC continues to use the definition of BES as 100 kv or higher then a Distribution provider would not be under this jurisdiction. Alternatively, what if a Distribution Provider can load shed >300 MW of power? Are they now included? These are very key considerations -- especially with the new use of smart meters/smart grid technology.
SDGE	In general, we feel that the CIP Standards should not be applicable to the Distribution System or Distribution Providers. The transmission system benefits the most from the requirements in the CIP Standards.
APPA	The APPA Task Force recommends substituting DP for current applicability to LSEs. LSEs do not own BES facilities. The DP may own certain very limited BES assets, generally limited to UFLS and UVLS relays. Associated BES Cyber Systems used to control the operation of these relays or transmit relay operations data to higher level entities (generally, the Transmission Operator) may properly be subject to BES classification under proposed CIP-002-4.
Consumers	Comment #1: We do not have any suggested criteria for DP or RA, but believe that if the SDT is unable to identify any specific criteria then these two entities should be removed from the standard. Comment #2: We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10

Organization	Question 11 Comments for DP (Response page 23)
NPCC	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.
MPPA	MPPA has concern expanding the applicability to Distribution Provider's. Any BES asset a DP may have should be sufficiently covered by the attachments. Adding DP's will not add value or increase the reliability of the BES.
Central Lincoln	While DPs own electrical assets, those assets are not considered to be within the BES. They should not be included.
NERC	Distribution Providers should be included on the list to acknowledge their support for load shedding functions. While directed by the Transmission Operator, oftentimes, the Distribution Provider is the practical implementer of the request and may have Cyber Systems that support this important BES activity.
Dominion	Do not add "Distribution Provider" to the list. By definition, Distribution is not part of the BES.
Dyonyx	Inclusion of Distribution Providers does not appear to be applicable to the intent of this Standard.
Oregon PUC	No comment
Manitoba 1	depends on the affect I assume on the BES.
Portland GE	No comment at this time
PSEG	Comment #1: We do not have any suggested criteria for DP or RA, but believe that if the SDT is unable to identify any specific criteria then these two entities should be removed from the standard. Comment #2: We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES.
WE-Energies	Wisconsin Electric Power Company agrees with EEI's suggestions regarding this question.
Idaho Power	Not appropriate to include. Minimal to no impact on the BES. Expands the scope beyond the BES.
SOCO	The DP function should not be added to the CIP standards at all.
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional entity should not be applicable to this standard.
Calpine	Doesn't appear to affect the functionality of the BES
Flathead	Opposed. This regulatory scheme was not intended to regulate local distribution, but continues to do so beyond FERC intent or authority. NERC/FERC directive for revising this set of standards was primarily directed at TO/TOP/GO/BAs that did not identify enough critical assets, not at LSE/DPs that didn't identify critical assets.

Organization	Question 11 Comments for DP (Response page 23)
E ON	Distribution is usually 69 kV and below, which is not BES (>100kV). Hence, they should not be added. Moreover, Section 215 (a)(1) provides that facilities used for distributing electric energy do not comprise part of the bulk power system. Sections 215(a)(2) & 215(a)(3) provide that the ERO and standards developed by the ERO address the Bulk Power System only. Cyber systems that are associated with both distribution facilities and BES subsystems should, by virtue of being associated with BES subsystem, already fall under the requirements of the standard. There is no need to include cyber systems associated solely with distribution facilities.
Carthage	Can this function impact the BES in real time? If so, please explain how.
Entergy	If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see Comments under Question 13.
CenterPoint	CenterPoint Energy does not agree with expanding applicability of this standard purporting to address Bulk Electric Reliability to Distribution Providers. The functions assigned to Distribution Providers by the NERC Standards are generally limited to load shedding functions, which are addressed by the currently CIP-002 standard through consideration of assets that shed 300 MW or more through a common system.
NIPSCO	We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10. We do not have any suggested criteria for DP, but believe that if the SDT is unable to identify any specific criteria then this entity should be removed from the standard.
ConEd	Yes, the standard should apply to the extent that UFLS or UVLS programs are under the control of the DP.
EEI	Distribution Providers should have applicability to the standard only if they operate transmission protection equipment or Special Protection System (SPS)
Alliant	We believe this Standard should only apply to Distribution Providers that own/operate BES assets
Ameren	SDT should provide reasons to include these entities as we have not seen any evidence to include these entities.
Black Hills	Should not be included.
NVEnergy	There is no reliability justification to include distribution providers as applicable entities.
SWTC	Will this require a entities to register as a Distribution Provider if they are not in the NERC Registry?
SCEG	none
Exelon	Exelon believes that the DP function should be added and LSE function should be eliminated from this standard applicability.
BPA Trans	None

Organization	Question 11 Comments for DP (Response page 23)
HQT	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.
KCPL	Depending on the criteria established, it is a possibility.
MidAmerican	Standards should be applicable to distribution providers and load serving entities if they own BES assets that meet the criteria for the BES as defined by NERC.
CPG	No comment
Santee Cooper	Would only include a DP if they own facilities that would cause BES outages.
OGE	• Inclusion of the Distribution Provider would require a significant lead time, resources and financial investment. • What authority does a Reliability Assurer have to regulate a distribution provider?
Oncor	We feel this Standard should only apply to Distribution Providers that own/operate BES assets.
NGRID	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added.
MGE	Only if the DP own BES assets under the definition of what a Distribution Provider is. If the DP did own or operate BES assets, wouldn't they be registered as a TO or TOP?
FE	"Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS.
TECO	We do not support the addition of DP.
CECD	Should not be included.
MRO	We feel this Standard should only apply to Distribution Providers that own/operate BES assets.
GTC	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Xcel	We feel this Standard should only apply to Distribution Providers that own/operate BES assets
BGE	We believe that Distribution Provider should not be included at this time as an applicable entity for this standard.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.

Organization	Question 11 Comments for DP (Response page 23)
FPL	We feel that expanding it to any facility is not necessary as this does not meet the definition of the BES.
TAPS	See TAPS response to Question 1.a.
Allegheny Power	Distribution Provider and Load Serving Entities should have applicability to the standard if they operate transmission protection equipment or Special Protection System (SPS).
FMPA	DPs are probably more important to include than LSEs. LSEs usually do not control breakers for instance, where DPs often do. The same criteria should be used for all Entities because the bottom line is avoiding “instability, uncontrolled separation, and cascading”, which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs.
Duke	They should be included if they have a Cyber System that could be exploited to impact BES reliability.
NBSO	Distribution Providers (DPs) should be added to the list of applicable Functional Entities, if registered for BES activities. Additional criteria for DPs should be added. DP's with a common control system or Cyber Asset that can impact a significant amount of load may not be captured in the registration process yet have impact.
AESI	Applying CIP to Distribution Providers is both undesirable and unnecessary. Existing CIP Standards already require Transmission related entities to protect their cyber assets from external entities, including Distribution Providers. There may be reasons for Distribution Providers to implement cyber security protections in specific cases (such as in connection with national security locations), but those reasons are unrelated to BES reliability and therefore should not be a reason to apply these standards.
Manitoba 2	Due to the potential impact that centralized control of a large number of distribution assets could have on the reliability of the BES, Distribution Providers should be considered within the scope of these standards.
OMPA	All Distribution Providers or only those that own and operate BES assets?
ATC	Do not add the Distribution Provider because entities with this registration have responsibility for distribution systems, rather than the BES. If an entity has responsibility for the BES reliable operation, then they would be registered as a Transmission Owner or Transmission Operator.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn’t this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren’t we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

<table>
<tr><th>Organization</th><th>Question 11 Comments for DP (Response page 23)</th></tr>
<tr><td></td><td>
It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable – Private</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Only if they own SPS.</td></tr>
<tr><td>IMPA</td><td>IMPA does not believe that a Distribution Provider should be added unless an engineering analysis shows that it has an Adverse Reliability Impact on the BES.</td></tr>
<tr><td>PacifiCorp</td><td>Comments on adding Distribution Provider: The standard should apply to Distribution Provider and if they operate transmission protection equipment or a Special Protection System (SPS).</td></tr>
<tr><td>PEPCO</td><td>Distribution Providers should have applicability to the standard only if they operate transmission protection equipment or Special Protection System (SPS)</td></tr>
</table>

Organization	Question 11 Comments for DP (Response page 23)
NEI	Some believe DP should have applicability, some believe they should not. "Applicability" of LSEs and DPs should be qualified according to whether LSEs and DPs own/operate facilities that are BES or support reliable operation of the BES, like UVLS/UFLS/SPS. However, when considered, if their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see #9.

Summary Consideration for Reliability Assurer: Most respondents felt that the Reliability Assurer could be excluded (pointing to the fact that the RA is not included in the NERC Glossary and confusion over how compliance for NERC and Regional Entities could be measured). The SDT agrees that the Reliability Assurer can be excluded, especially now that there is no requirement that directly references Reliability Assurers.

Organization	Question 11 Comments for RA (Response page 23)
Progress Energy	NERC needs to define Reliability Assurer.
GSOC/OPC	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Consumers	Comment #3: We do not believe that DP adds value. RA may add value in regards to information protection / information assurance.
NPCC	Recommend that Reliability Assurer not be added to the list of applicable Functional Entities. NPCC does not provide real time operational input.
Central Lincoln	This standard is about classifying cyber subsystems, not registered entities. These entities do not own the assets in question, so they should not be included.
Dominion	Add “Reliability Assurer” to the list. Since Attachment 1 requires an “engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer” there should be a requirement imposed on these entities to develop criteria for each. See comment to item 4 above.
USBR	Reliability Assurer is only defined in the Reliability Functional Model and is not included as a defined term in the Glossary of Standards. This treatment is inconsistent with the other functions. The term will need to be defined in order to be used in the Reliability Standards. It is not cleat that the role is needed in this standard.
Green Country	Who, what, when, where, why and how....?? Never heard of this function
Oregon PUC	No comment
Manitoba 1	No comments
Portland GE	No comment at this time
PSEG	Adding the RA functional entity type would be as described in question #10. Comment #3: We do not believe that DP adds value. RA may add value in regards to information protection / information assurance.
WE-Energies	Wisconsin Electric Power Company agrees with EEI’s suggestions regarding this question.
Idaho Power	Need a definition of what this function is. This would seem to be a responsibility of all the registered entities.
SOCO	Currently we don’t know who this is. Not being defined in any approved functional model.

Organization	Question 11 Comments for RA (Response page 23)
DTE	If criteria are not defined, the entities should be removed from the applicability section.
AEP	This functional role is not yet approved or in effect.
Calpine	The definition of Reliability Assurer is unclear to us.
Flathead	This should be Regional Reliability Organization or Reliability Coordinator.
E ON	It is unclear to E ON U.S. what this term means. “Reliability Assurer” is not in the NERC Glossary of Terms neither is it defined in this draft standard. E ON US objects to the inclusion of this term.
Carthage	No comments
Entergy	If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see Comments under Question 13.
CenterPoint	The term of Reliability Assurer needs to be defined.
NIPSCO	We have concern over expanding applicability to additional functional entities. For end use customers who are served at transmission voltages, the transmission owner would already serve as the distribution provider. Adding the DP function would not gain any new applicability in relation to the BES. Adding the RA functional entity type would be as described in question #10. We do not have any suggested criteria for RA, but believe that if the SDT is unable to identify any specific criteria then this entity should be removed from the standard.
ConEd	Yes, since the Reliability Assurer has a role in reviewing and approving models and engineering studies.
Alliant	Reliability Assurer needs to be adequately defined before we can make a judgment on this.
Black Hills	RA's should be included.
NVEnergy	The functions of a Reliability Assurer do not include the ownership or direct operation of BES facilities; therefore this standard should not be applicable
NCEMCS	Given the high probability that DP facilities would all fall under the low impact category, this inclusion would do very little to benefit the reliable operation of the BES but would add significant cost to distribution co-operatives and ultimately their end user members.
SCEG	none
Exelon	No comment
BPA Trans	None
HQT	Recommend that Reliability Assurer should not be added to the list of applicable Functional Entities. NPCC does not provide real time operational input.

Organization	Question 11 Comments for RA (Response page 23)
KCPL	No comments
MidAmerican	Reliability Assurer is not in the NERC Glossary of Terms. MidAmerican's proposed changes to CIP-002-2 eliminate the need for a reference to Reliability Assurer.
CPG	No comment
Santee Cooper	none
NGRID	National Grid recommends that Reliability Assurer should not be added to the list of applicable Functional Entities.
MGE	This is undefined, the question cannot be answered.
TECO	It is not clear to us what BES subsystems would apply to an RA, therefore we cannot make a determination on this.
CECD	Should be included.
MRO	This is difficult to ascertain without knowing the formal definition of a Reliability Assurer. We feel these needs to be defined in the NERC Glossary of Terms.
GTC	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Xcel	This is difficult to ascertain without knowing the formal definition of a Reliability Assurer. We feel these needs to be defined in the NERC Glossary of Terms.
BGE	This term should be included in the "NERC Glossary of Terms used in Reliability Standards."
FPL	This function is not yet FERC approved. See previous comments on this matter.
TAPS	See TAPS response to Question 1.a.
FMPA	The same criteria should be used for all Entities because the bottom line is avoiding "instability, uncontrolled separation, and cascading", which are caused by certain known technical criteria – supply / demand mismatch and exceeding IROLs. It is unlikely that the RA will have any such Cyber Systems.
Duke	They should be included if they have a Cyber System that could be exploited to impact BES reliability.
AESI	Based on their role as defined in the NERC Functional Model, RAs may have significant amounts of information which needs to be adequately protected. The best way to provide this protection may or may not be via the CIP standards.
Manitoba 2	We are unfamiliar with the term "Reliability Assurer" and are unable to comment.
OMPA	Cannot comment; unsure of the definition of "Reliability Assurer".

Organization	Question 11 Comments for RA (Response page 23)
ATC	Do not add the Reliability Assurer because we understand these entities to have responsibility for monitoring compliance with the reliability standards requirements. So, they should be accountable for requirements that they are responsible for monitoring (e.g. conflict of interest). In addition, we understand that registration for the Reliability Assurer has not been established yet.
IMPA	IMPA might see where this entity could be added to ensure approvals of engineering evaluations or other assessment methods are performed in a timely manner and equally across the region or the country.
ERCOT	ERCOT ISO reads the applicable Function Entities list to not include the “Reliability Assurer”. Further, there is ambiguity as to what organizations would be registered as a Reliability Assurer. This is an active discussion item with the Functional Model Working Group.
PacifiCorp	Comments on adding Reliability Assurer: Reliability Assurer is not a term defined in the NERC Glossary of Terms.
NEI	This functional role is not yet approved nor in effect. When the role is approved and in effect, CIP 002-4 should apply (note that they have a function for performing or reviewing Engineered Evaluation already). If their cyber assets are conjoined on a TCP/IP network infrastructure with those of other BES Responsible Entities, e.g., via NERCnet, then the same cyber impact categories analogously should apply – see #9.

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

Summary Consideration: Many respondents reiterated that the focus for these functions should be cyber systems that support real-time operations. Many found issue with the "include, but are not limited to" section of the functions. Others commented that attachment 2 is confusing and should be eliminated. Comments were made about unintended reliability effects, citing blackstart units as high impact, and therefore could result in reduction of these units. Commenters also wrote that the examples should be moved to a guidance document. One commenter noted that attachment 2 has a wider application and does not belong in a CIP standard.

The SDT has clarified the scope of the functions and removed all the examples. The former attachment 2 is a necessary attachment to define the scope for BES Cyber Systems and the functions they support.

Organization	Question 12 Comments (Response page 24)
Progress Energy	Tools that are used in the planning horizon are not critical to BES reliability and should be removed from the proposed functions. (e.g. Unit Commitment under Balancing Load and Generation.) The focus for these proposed functions should be cyber systems that support real-time operations.
GSOC/OPC	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems might have on the BES and subsequently the impact which should be assigned to them.
Hayden	In the July 21, 2009 NERC Concept Paper "Categorizing Cyber Systems An Approach Based on BES Reliability Functions," there is a list of BES functions that is not identical to the list in CIP-002-4 Attachment 2. As a suggestion for consistency and to take advantage of the thoroughness of the info in the Concept Paper, why not use the nine functions identified in Figure 1 and Table 1 which include: 1) Contingency Reserve/Peakers; 2) Load Balancing, Frequency Response/Support; 3) Voltage Support/Reactive Power Supply; 4) Constraint Management; 5) Control and Operation; 6) Situation Awareness; 7) Restoration; 8) System Stability; 9) Load Management
Consumers	Attachment 2 is a listing of high-level tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
NPCC	Please clarify "control" in 6 – Control & Operation. Recommend adding parameterization, calibration to 6 – Control & Operation. Suggest that the words for 8 - Situational Awareness should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES." Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function

Organization	Question 12 Comments (Response page 24)
	includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications". Existing language would include voice communications. Attachment 2 is not careful as to whether it applies only to BES Elements. If it is taken to apply to any Element then it becomes a definition of the BES System.
Central Lincoln	Make the list complete. The "include, but are not limited to" open ended function list leaves too much room for disagreement.
Dominion	Dominion has the following suggestions: 1. Dynamic Response – Dominion disagrees with the inclusion of Spinning Reserve and Governor Response as neither of these is dependent upon a cyber system. 2. Balancing Load and Generation – Dominion disagrees that any of the listed activities is solely dependent upon a cyber system. These functions can be performed without employing a cyber system. The listed activities should only be included if they are solely dependent on computer systems, intranet or internet to allow access to multiple parties. 3. Restoration of BES – Dominion disagrees with including this function, as most restoration plans assume the transmission operator's system has suffered a total blackout. It is extremely doubtful in this case that any cyber systems will be used, because each step of the process will have to be manually tracked. Inclusion should be determined on a case-by-case basis based upon the specific restoration plan.
Encari	We recommend reviewing for inclusion the following critical functions: 1. Emission systems (with indirect impacts) 2. Remote Cyber Support
USBR	Dynamic Response Section Spinning Reserve is listed which by itself is not an automatically triggered and not a Dynamic Response quantity. Units, or capacity so designated, is controlled by AGC. Governor Response should specifically mention AGC. Unless its control is addressable, Governor frequency response should not be included as a part of the Cyber standard. Excitation Systems with Automatic Voltage Regulators are not listed and should be. Under and Over Frequency Relay, Under and Over Voltage Relays are covered under Protection Systems. To call them out separately implies otherwise. AGC should not be listed in the Controlling Frequency section as it is a Dynamic Response. This Controlling Voltage section does not list "Transmit adjustments to individual units" (in response to a voltage schedule). The Control & Operation section needs to include Generator controls for AVR, and AGC.

Organization	Question 12 Comments (Response page 24)
	The Situational Awareness section is covered by the other sections and is not needed.
Westar	Attachment 2 only adds confusion and should be eliminated.
Green Country	Clearly identify if for each function if you need all of the elements below it or just one, to be considered having that function. For example if all you have is power system stabilizers, do you have the Dynamic Response function?
Oregon PUC	No comment
Manitoba 1	No suggestions
Portland GE	No comment at this time
PSEG	Comment #1: Attachment 2 is a listing of high-level tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
WE-Energies	In general, there's a mix of prescriptive and non-prescriptive items under each of the categories (include but are not limited to ...). The definition of dynamic response is confusing. Wisconsin Electric Power Company recommends combining 2, Balancing Load and Generation and 3, Controlling Frequency into one category.
Idaho Power	Attachment 2 supports the identification of cyber systems that support critical BES functions but seems to suggest by the title of the attachment that all functions being critical are also high impact and therefore does not assist with the categorization of assets that could potentially be medium or low impact.
SOCO	There are several places where the proposed standard could have unintended consequences with negative effects on reliability. For example, the requirement that all blackstart units registered as part of the regional reliability plan be classified as high-risk could lead to Entities reducing the number of declared blackstart units; an exemption based on an approved engineering study should be allowed. Under many of the 9 categories of functions (i.e. Dynamic Response, etc.) there is a phrase that states “Aspects of BES Dynamic Response include, but are not limited to:”. We feel that “but are not limited to” is too broad and should be deleted. This Standard attempts to establish requirements for a very broad array of equipment and systems having very different functions and vulnerabilities dependent on the physical installation, usage and method in which they are connected. An example is the use of alarms. Controls Centers tend to have a high number of critical alarms with few low priority alarms, while a Generation Unit could have thousands of alarms with the majority being lower informational type alarms. Some of the alarms within a generating unit are prioritized and used for the indication and alerting of non-operation personnel such engineering or maintenance use. A second area is the physical installation configuration of an area. Generation units are typically in continuously manned and guarded location, transmission facilities may be in non-manned and isolated areas. Control Centers are located in a smaller, office type environment, which is more readily enclosed in “six wall” confines. Consideration should be given to moving Attachment 2 to a FAQ document divided into sections discussing the following areas:

Organization	Question 12 Comments (Response page 24)
	• Control Centers • Generation Units • Transmission Facilities Attachment 2 1. Dynamic Response - Generator governor controls may be purely mechanical or local electronic controls without connections to remotely accessible systems. Attachment 2 2. Balancing Load and Generation - This section should be clarified to address the balancing of electrical system load vs. electrical system “supply”. It could be interpreted to apply to the pure generation unit control aspect. Is “Manually Initiated Load shedding” the area of interest or the ability to identify. If “identify” this is under the scope of Situational Awareness in Item 8. Attachment 2 8 Situational Awareness - A definition or the intent of “Change management” should be included. Is this the management of change as cover in other sister standards? Suggest that Attachment 2 refer back to engineering studies to determine the level of impact these functions have on the BES for categorization.
DTE	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Functional Model or the Definition of Adequate Level of Reliability.
AEP	This is a very good request in that it seeks the increased clarity that we see as needed in the functional descriptions. AEP believes that this standard needs to be segmented into each applicable function and not try to use a “one size fits all” approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.
Flathead	The situational awareness, control and operations, criteria are so broad that they would include small call centers and local distribution entities that don't have a "control center" under current standards, but might under these standards.
E ON	E ON U.S. recommends the team revisit what is a switch from identifying critical assets to identifying critical BES functions and then requiring the as yet undefined requirements of CIP-003-009 V4 be applied to associated assets. Generating units, RTUs, communications lines and the like are all subject to being out of service, forced or scheduled, yet BPS reliability is maintained. Attachment 2 makes no allowance for system diversity and redundancy Attachment 2 lists monitoring of spinning reserves which requires telemetry from every generating unit. This implies that every generating unit, regardless of size, falls under this standard. This would also seem to include each RTU and all the communication equipment back to the EMS. E ON U.S. has the same concern regarding calculation of ACE. This implies that all communication equipment back from the RTU for every input into the ACE equation. The drafting team should clarify item 5 “Managing Constraints” of Attachment 2. Could this include cyber assets used in the calculation

Organization	Question 12 Comments (Response page 24)
	of ATC? Tagging systems used to submit schedules?
Carthage	CWEP feels that Attachment 2 should be eliminated because it causes confusion. CWEP feels that the functions should be specifically covered in Attachment 1 under the impact categories they fit. The way the attachments are designed leaves too much room for interpretation. CWEP is okay with the format of the standard but would like for the criteria to be more specific. Is the bullet under number 1 that deals with under and over frequency relay protection intended for all entities that participate in under or over frequency load shedding or just the bigger entities as stated in Attachment 1 section 1.14? CWEP feels that applicability needs to be clarified throughout the standard to ensure that it's interpreted correctly. If under or over frequency load shedding are considered critical to the reliability of the BES, it should be clearly defined in the criteria for the impact categories of Attachment 1 what levels of load shedding fit each category like 1.14 of Attachment 1.
WECC	No suggestions, purposed attachment 2 looks comprehensive and well thought out.
Entergy	None
CenterPoint	Function #8 – Situational Awareness is too broad and needs to be better defined. In particular, the "change management" aspect of Situational Awareness is unclear.
LCRA	1. Attachment 2, 8, bullet 2 – Change management should be better defined or removed from the list. 2. Attachment 2, 8, bullet 5 – Frequency monitoring should be better defined so that the loss of a single monitoring point in a many point scheme is not a problem.
NIPSCO	Attachment 2 is a listing of tasks performed by NERC functional entities. The standard already covers the assignment of applicability to functional entities and restating a select subset of the tasks performed by the functional entities seems redundant.
ConEd	Cranking Path should be clearly defined for application in this Standard.
EEI	Replace "Functions Critical to the Reliable Operation" with "Functions that Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances.
O&R	Cranking Path should be clearly defined for application in this Standard.
Alliant	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternate title "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems. Please provide the basis for including each of the items listed.
Ameren	Attachment 2 is overly broad, e.g. managing ATC, situational awareness, etc.
Black Hills	Not at this time.

Organization	Question 12 Comments (Response page 24)
TNMP	TNMP has concern with creating a definition and then supplementing the definition with an Attachment providing additional criteria and clarification of a term, as addressed with the High BES Impact comments. If a person were to just look in the NERC glossary then they would have no idea there were additional criteria defining a BES Cyber System. If an appendix or attachment is necessary, the definition should clearly reference the additional information. In TNMP's opinion the drafting team needs to review the definition of "BES Cyber System" to ensure the desired clarity and certainty for inclusion and consistency are obtained.
NVEnergy	Items 2 and 3 are so closely related that they should be combined (Balancing Load and Generation, Controlling Frequency).
MWDSC	Clarify functions that are critical to reliable operation of interconnected BES, not isolated BES Subsystems.
Empire	If you identify a control center in attachment 2 then this is not needed.
SWTC	THE BES Task Force needs to set the criteria for BES before this Standard can have merit.
SCEG	Suggest adding "Voltage Regulators" to 1. Dynamic Response list.
Exelon	None
BPA Trans	None
HQT	Suggestions for improving proposed functions: Please clarify "control" in 6 – Control & Operation Recommend adding parameterization, calibration to 6 – Control & Operation Suggest that the words for 8 - Situational Awareness should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES." Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications". Existing language would include voice communications. Attachment 2 has potential for wider application and does not belong in a CIP standard.
Allegheny Energy	Definitions need to be clarified (e.g.): "Governor Response" - is this movement of a governor to respond to frequency deviation? "Providing Actual Reserves" - Are these systems that request additional generation in response to an event?
KCPL	The criteria proposed in Attachments 1 and 2 are too broad to provide sufficient substance required to provide the industry with

Organization	Question 12 Comments (Response page 24)
	meaningful guidance. What is the engineering basis for the generator levels and transmission voltages for High and Medium? I recommend the CIP Drafting Team consider the establishment of an engineering team to develop the criteria to "plug into" this Standard to provide substantive and meaningful criteria for determining reliability impact of facilities.
MidAmerican	The nine functions defined in attachment 2 are confusing, too broad and will have different meanings for different entities. It will be difficult to implement and audit using Attachment 2 as proposed. Eliminate attachment 2. Retain the concept of Critical Cyber Asset. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. If needed, instead of creating Attachment 2, provide additional bright line specificity for the Cyber Assets expected in existing CIP-002-2 R3.
CPG	The prior version of CIP-002 considered two dimensions of risk. The first dimension of risk considered was impact, which was whether or not a cyber asset was associated with a critical asset. Secondly, it considered vulnerability by determining whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal, the SDT has eliminated any consideration of the risk due to vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest categories of varying degrees of vulnerability (high and low) be added to the criteria in Attachment 2.
Santee Cooper	None
Oncor	Item 8 – Situational Awareness. What does "Change management" mean? Please explain it, or delete.
NGRID	• Replace "Functions Critical to the Reliable Operation" with "Functions that May Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances. • Please clarify "control" in 6 – Control & Operation • Recommend adding parameterization, calibration to 6 – Control & Operation • In 8 - Situational Awareness, suggest these words should be consistent with the real-time operations words for situational awareness in the Control Center definition. • Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational

Organization	Question 12 Comments (Response page 24)
	decisions regarding the reliability and operability of the BES." • Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications"
MGE	Upon review of the Functional Model, there are some items that are contained in Attachment 2 that fall outside of the Functional Model. Please provide the basis of these items. Please clarify that only High and Medium BES Impact items are to be used in Attachment 2, since items listed in the Low BES Impact category do not have the potential to adversely affect the BES.
TECO	We believe that the list of functions in Attachment 2 is overly broad and will introduce many systems that do not have a direct impact on the reliable operation of the BES subsystems. Please see our previous comments in questions 2 and 6. We are particularly concerned with the Situational Awareness. For example, systems that report on the capability and status of various units for next day planning, if unavailable will not directly impact the reliability of those BES subsystems that they support, and could be easily tracked on a spreadsheet. We are also concerned with Balancing Load and Generation, specifically, the sub heading of Unit commitment. For example, a simple spreadsheet showing the capabilities of generation units (including High, Medium and Low BES Impact Units) that will be used by management for purely informational purposes has no impact on the BES and should not be considered a High Impact BES Cyber System (according to R3.2). Under Situational Awareness: It is unclear whether Change Management applies to IT Systems or change management as it relates to other work being performed on BES subsystems, for example repairs during a unit outage, or replacement of substation equipment. Additional Attachment 2 Questions: "2. Aspects of the Balancing Load and Generation function include, but are not limited to: Load management – Ability to identify load change need – Ability to implement load changes • Demand Response – Ability to identify load change need – Ability to implement load changes " These functions may be outside the Control Center. It is not clear if the intent would be to expand scope beyond the control center.

Organization	Question 12 Comments (Response page 24)
	5. Managing Constraints "Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES." Is the intent to pull systems such as Oasis and OATT into scope under managing constraints?
MRO	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternative title of "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems". We would also appreciate if the Standard Drafting Team could provide the basis for including each of these items.
GTC	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems might have on the BES and subsequently the impact which should be assigned to them.
Xcel	In and of themselves, not all of these functions are critical to the reliable operation of the BES in all cases, so we propose an alternative title of "Functions Utilized for the Reliable Operation of Bulk Electric System Subsystems". Flexibility needs to be incorporated into these definitions to allow exclusion of cyber systems that are not critical to the operation of the BES Generation or Transmission Subsystem. Failure or compromise of some cyber systems may not impact the operation of the subsystem for a significant length of time, allowing for repair. These systems should be excluded from the standard. For example, a PC based coal receiving unloading system. The fuel inventory on-site will supply the plant for a number of days, weeks or months depending upon the amount in inventory." No reliability improvement would be gained from applying cyber controls to this system. We would also appreciate if the Standard Drafting Team could provide the basis for including each of these items
BGE	The prior version of CIP-002 considered two dimension of risk. They considered impact, whether or not a cyber asset was associated with a critical asset. And they considered vulnerability, whether a cyber asset was accessible by dial-up or routable protocol, or if it was not. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal the SDT has eliminated any consideration of the dimension of vulnerability from the standard. It is doubtful that the goal of a establishing practical and appropriate controls can be done without it. We would suggest that various categorization of vulnerability be designated in CIP-002 (High, Medium, Low or High, Low, No?) and the sorting criteria be established in an appendix, similar to Attachment 1 that correspondingly deals with the dimension of impact.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question.
FPL	Not at this time
TAPS	See TAPS response to Question 1.a.
Allegheny power	AP suggests eliminating Attachment 2.
FMPA	FMPA would beg to differ on the wording of the question, Attachment 2 does not contain functions "critical" to the reliable operations of

Organization	Question 12 Comments (Response page 24)
	the BES, but rather activities to maintain the reliable operation of the BES. FMPA recommends eliminating Attachment 2 altogether or creating a supporting paper of “things to consider”, or at most, a bullet item list in the requirements of the standard of “activities to consider when evaluating worst case scenarios / contingencies that can be caused by malicious use of a cyber system” If the SDT insists on keeping Attachment 2, then it needs to be much less ambiguous. For instance, for Situational Awareness, is a single transducer going out of calibration a loss of Situational Awareness? And the focus should NOT be on what can compromise the items on this list, but, on the level of risk of an Adverse Reliability Impact as a result of compromising the items on the list. Therefore, most of these functions are NOT functions critical to the reliable operation of the BES. A protection system on a single transmission line that is not part of an IROL is certainly NOT critical. A governor response of a single generator is certainly NOT critical. A single UFLS or UVLS relay is certainly NOT critical. A single Power System Stabilizer is certainly NOT critical. Calculation of ACE is certainly NOT critical. Etc., Etc. This standard should focus on what is truly critical, threats of an Adverse Reliability Impact of “instability, uncontrolled separation, or cascading”.
Duke	In addition to identifying functions that impact BES reliability, it should also address categorizing the risk associated with different types of Cyber Systems (i.e. systems that are part of a routable protocol control system network have higher risk than those which utilize serial or dial-up communications), etc.
NBSO	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.” to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline
AESI	Attachment 2 provides a list of the functions which a Cyber System has to be capable of adversely impacting in order to be considered a BES Cyber System, however it does not address the varying levels of vulnerability and impact which a given set of BES Cyber Systems might have on the BES and subsequently the impact which should be assigned to them.
Manitoba 2	The term “functions critical” should be changed to “functions essential”. The functions list is fairly comprehensive.
OMPA	For Item 6: Control & Operation; OMPA suggests the example should include “electronic” control rather than “all” control.
ATC	Replace “Functions Critical to the Reliable Operation” with “Functions that May Affect the Reliability of the Operation”. This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances. Item 8: - Change management - Current Day and Next Day planning

Organization	Question 12 Comments (Response page 24)
	What is the team attempting to identify with these items? They both could be interpreted to mean outage scheduling applications.
LES	We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links. It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact: (the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)

	Security Function						
Network Connections	Physical Perimeter	Data Encryption	Antivirus	OS Patches	Intrusion Detection	Account Passwords	Firewall
Air Gap	✓						
Non-Routable – Private	✓						
Non-Routable -Public	✓	✓					
Routable - Private	✓		✓	✓		✓	✓
Routable - Public	✓	✓	✓	✓	✓	✓	✓

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that "physically" isolate systems (i.e. unidirectional communications), but the current "flavor" of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an "air gap" solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is

Organization	Question 12 Comments (Response page 24)
	being coerced into standards that don't follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the "Aurora Vulnerability" which was misrepresented as a cyber attack, when it really wasn't (see the NERC MRC presentation for Feb. 15th, 2010).)
PSE	Will look to review further in the next draft as more specificity is detailed.
IMPA	IMPA does not believe all of the functions listed in Attachment 2 will always be critical to the reliable operation of the Bulk Electric System. The title of the document should be changed to reflect this issue by eliminating the word critical.
ERCOT	In Attachment 2, Section 3 we assume that it was intended to state "but are not limited to".
PacifiCorp	The nine functions defined in attachment 2 are confusing, too broad and will have different meanings for different entities. It will be difficult to implement and audit using Attachment 2 as proposed. PacifiCorp proposes eliminating Attachment 2 on the basis that the concept of Critical Cyber Asset should be retained as security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." The qualifying criteria that consider routable protocol or dial-up accessibility should be retained because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. If needed, instead creating Attachment 2, provide additional bright line specificity for the Cyber Assets expected in existing CIP-002-2 R3.
NEI	A) Revise to consider cyber first, then the impact to the BES. B) Dynamic response not considered – Don't require cyber systems to balance load and generation. C) There is a concern with the matrix of cyber vs. BES: Something with high cyber impact may have no impact on BES and something with high impact on BES may have no cyber impact. This is not a 1:1 relationship, yet it appears to be treated as such. D) This standard needs to be segmented into each applicable function and not try to use a "one size fits all" approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.

13. Do you have any other comments to improve the draft standard?

Organization	Question 13 Comments (Response page 25)
Progress Energy	In Attachment 1, propose removing "1.2 - Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations." Need clarification on why this criterion was chosen as a High BES Impact.
EPSA	The Electric Power Supply Association (EPSA) appreciates the opportunity to comment on Standards Drafting Team's (SDT) revisions to the Critical Infrastructure Protection (CIP) Standard 2, Version 4 regarding Critical Asset Identification for Bulk Electric System (BES) assets for Cyber System Categorization. The BES serves as the essential highway for competitive generators to cost effectively deliver electricity to customers. Moreover, the development of the CIP standards is essential to ensuring grid security and reliability for electricity customers. I. Background and Overview Competitive suppliers recognize the SDT's challenge of balancing traditional societal electricity goals of reliability and reasonable costs with a new goal -- security. EPSA strongly supports the principles that the SDT seeks to achieve by protecting the BES through the prevention of system instability, prevention of critical subsystem separation and ensuring against cascading outages. Therefore, EPSA is providing additional criteria that the SDT should include in the standard to better link the tiered approach with the articulated principles. The electric power industry is the most capital intensive industry in the U.S. Electric generation is the bulk of this investment, representing more than 70 percent of the average consumer's bill. It appears that it is NERC's view that there should be more generators identified as critical assets. However, NERC has not provided any link between imposing additional regulation/costs on a broad swath of additional generation and accomplishing the identified principles. These goals will be best accomplished if NERC issues specific and transparent criteria that identify generation facilities that are truly critical to maintaining BES reliability and then use the industry's expertise to develop cost-effective measures focused to address any identified threat. Thus far the efforts of the SDT have produced useful foundations to help shape a revised set of CIP standards. However, the addition of a sound basis from which to build a structure must also include a cost benefit analysis that is a fundamental tenet of NERC standard development. In addition, it is very difficult to establish the High, Medium, or Low BES impact without the benefit of knowing what the resulting CIP-003 through CIP-009 standards will be. Linking the standard criteria to the reliability and security needs, will enable industry to craft an effective set of cost effective, reliability focused measures. Failing to steer the efforts around a reasonable basis could impose unreasonable costs and produce perverse incentives that may run contrary to reliability goals. Furthermore, the SDT must recognize that it very difficult for an independent generator to fully access whether or not it is critical to the bulk transmission system, and if so at what level. Simply put, generators do not have access to all of the information that is necessary to perform the comprehensive engineering analysis that should be utilized to identify critical assets and correct tier (i.e., High, Medium or Low). Thus it may be more appropriate to assign the obligation to identify critical generation to the Regional Entity (RE) or Reliability Coordinator (RC). Such entities have access to the system data necessary to performing such studies and to making such determinations. Such determinations should not be made in isolation, but in an open and transparent manner, pursuant to clearly defined NERC standards, and with an opportunity for impacted generators to fully participate in the decision process. II. Comments

Organization	Question 13 Comments (Response page 25)
	EPSA's membership supports the use of engineering analysis that is based on scenarios and reasonable assumptions. However, a high-level, bright-line approach is preferable to the SDT. EPSA's membership considered a broad range of potential metrics including geographic location, electric topography, generator performance statistics, and others for the SDT's consideration. Ultimately, while such criteria are useful and could be used to include/exclude some assets in a transparent matter, they are not a substitute for engineering and system operations analysis performed by the applicable reliability authority. EPSA supports the SDT's use of the term Generation Subsystems to define the BES critical assets that can then be categorized through a tiered - High, Medium, Low criteria. However, the concentration and location of generating assets and how that factors into grid topology must also be considered when determining a Generation Subsystem's level of impact. Grid constraints and contingencies play key roles in real-time grid operation, as well as during restoration, making the generation location a significant consideration in determining criticality of Generation Subsystems. In Appendix 1 of the draft standard the SDT provides a framework for how specific subsystems would be categorized. The framework, however, is in some cases subjective or arbitrary (i.e., megawatt level, voltage level, etc) whereas the definitions for High, Medium and Low impact are objective. For example, High BES Impact is defined with respect to preventing system instability, separation or cascade (ISC) whereas the test makes reference to an arbitrary 2,000 MW threshold. EPSA supports the ISC thresholds in the defined terms and suggests the standard be written so that more direct links can be made among the ISC and the tiered approach. EPSA members have discussed at length different threshold measures for determination of the three tiers defined by High, Medium and Low BES impact. Because a bright-line is considered necessary, capacity factor and nameplate capacity were initially considered. These are clearly important factors. However, when system operation and grid topology are considered, size and volume alone do not always provide sufficient linkage to grid reliability or security measures. While a large facility (i.e., greater than 100 MW) with a low capacity factor may not be critical to system reliability, this may also be a factor of the unit's start-up time or ramp rate. A smaller unit with a low capacity factor may be a peaking unit serving an important system reliability purpose. Simply put, nameplate rating and size did not provide a connection to how a generator impacts ISC. Thus, the definitions associated with the tiers and their importance does not provide a sufficient link to the tiered approach in Appendix 1. The location of a Generation Subsystem and how it integrates with the grid can have a much greater impact on ISC and, therefore, needs to play a role in the criteria. For example, a small peaker in New York City might have more significant impact on ISC than a similar facility in a remote area of Montana. Other factors also play a role in determining the relevant tier for a Generation Subsystem. The SDT should provide specific criteria for Black Start units (including units in the cranking path), Reliability Must Run (RMR) units, and possibly any units used to provide non-spin reserves. Since these units can be part of a subsystem, a precise definition for these units and plants will be necessary for identifying and categorizing specific assets. For example, under 1.3 - Pre-designated Reliability Must Run Unit – it is not explained how are units pre-designated. In organized markets will the designation be signified by a contract with the RTO/ISO and a specific utility in other regions? Will such a designation be dependent on the balancing authority? Also regarding 1.4 -Blackstart Generation Subsystem - if there are an excess of Black start units in a BA, are all a part of that Blackstart Generation Subsystem? Providing these distinctions will lead to greater Standard clarity. Another important factor that should be considered is whether, in the organized market regions, a unit has a capacity obligation (including a unit-specific bilateral contract with a load serving entity). While the presence of a capacity obligation certainly should not be litmus test for categorizing a unit as critical, any unit without a capacity obligation should not qualify as critical, even as "Low" level.

Organization	Question 13 Comments (Response page 25)
	Due to the important role the evaluation of a Generating Subsystem's regional location plays in determining its critical impact, EPSA is encouraged by the STD deference to REs playing a role in the determination of generating assets criticality. REs can best utilize other entities such as Reliability Coordinators -- so that appropriate transparent determination can be made. Moreover, the REs are in the best position to evaluate local grid considerations to prevent ISC events. While detailed criteria are appropriate and necessary to ensure consistent determinations of critical assets and tier assignments, an engineering analysis that examines system contingencies, as well as normal and emergency system operation, should be one of the criteria used in making most such determinations. Thus, the obligation to identify critical assets and to identify the appropriate tier must be placed where it belongs – upon the REs and Reliability Coordinators that have the information necessary to conduct a engineering analysis in a transparent manner and to make the determination. Footnote: EPSA is the national trade association representing competitive power suppliers, including generators and marketers. These suppliers, who account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities serving global power markets. EPSA's 21 member companies each operate in four or more NERC regions and represent over 600 registered entities in the NERC registry. The comments contained in this filing represent the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.
Dynegy	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. As a member of the Ballot Body, I will not even consider voting to approve this Standard unless Version 4 of CIP-002 and Version CIP-003 through CIP-009 are voted upon/balloted at the same time. We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA it is also registered as BA ? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation.
GSOC/OPC	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a

Organization	Question 13 Comments (Response page 25)
	new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards. 2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary? c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could be lowered if certain protective criteria were met (encryption etc.). 5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas

Organization	Question 13 Comments (Response page 25)
	should produce a superior set of standards. 6. With respect to section 4.1 of the Standard, the second sentence, beginning “In situations where . . . ,” should be deleted as unclear and unnecessary.
Hayden	1. I'd suggest that this standard also be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version be addressed completely (including recognition of consequences of new changes). 2. What about "non-routable protocols" and their inclusion/exclusion under CIP-002-4? For instance if you expand the standard to all protocols then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems" and as such this could be a large change to the Registered Entities that it would be difficult for them to become compliant. 3. The Frequently Asked Questions (CIP-002, Question 11) notes that communications systems are not included in CIP-002; however, the new definition of Cyber Systems now includes the "communication" element. Suggest expanding this discussion to address whether or not communications systems are included or not in CIP-002-4. 4. R2 of CIP-002-4 does a good job about having Registered Entities exchange information on BES systems to transmission system owners directly connected to the subsystem. Perhaps this would be a good opportunity to highlight rules/expectations for jointly managed facilities and how "memorandum of understanding" can also be prepared between these Registered Entities that address key requirements such as key responsibilities, definitions of physical and logical boundaries, etc. 5. Does CIP-002-4 change the original Frequently Asked Question response that HVAC, environmental systems are not included in the "Critical Assets" (now BES Cyber Systems)? 6. In question 13 of the FAQ for CIP-002 alarm systems are potentially excluded from the protection as a Critical Cyber Asset. However, with the new definition of a Cyber System, are alarm functions included? (As a note, if an alarm system is "hacked" or fails and results in operators not recognizing negative impacts to the BES, I would argue that these systems should be treated as Critical Cyber Assets.)
SDGE	Attached are suggestions to include for High BES Impact for Transmission Subsystem: - Substation is essential for regulation of Bulk Power voltage - Loss of the substation (all busses greater than 200 kV) may result in voltage less than 90% of nominal, or thermal overloads in excess of 110% of applicable ratings (to be studied at forecasted 50/50 annual peak loads) - Loss of substation may result in voltage collapse or non-localized cascading system outage resulting in more than 100 MW of load loss - Is the substation essential for black start restoration - Does the loss of the substation result in the loss of critical generation

Organization	Question 13 Comments (Response page 25)
	- Is the substation essential for frequency support (can it result in under-frequency load shed or frequency related instability) - Is the substation essential for stability (does the loss of a substation result in loss of resources greater than largest G-1; is the substation essential to an SPS needed to avoid instability, uncontrolled separation, or cascading outages) Attached are suggestions to include for High BES Impact for Generation Subsystem: - Is the generation essential for voltage support and frequency response (is it needed for voltage stability; can the loss of generation result in voltage collapse; can the loss of generation result in underfrequency load shed) - Is the generation essential for black start restoration In Attachment 1, section 1.6 refers to the Transmission Subsystem comprising Black Start Cranking Paths. Does this include 69 kV and 138 kV substations? In Attachment 1, section 1.13 and 2.5 state "… would have an Adverse Reliability Impact." Please define and if this refers to "High BES Impact", state as such. In Attachment 1, section 1.12, we recommend replacing "Cascading outages" with "non-localized cascading outages resulting in over 100 MW loss of load."
APPA	APPA Task Force Prefatory Comments: The APPA CIP Task Force supports the general framework for BES cyber-security proposed by the CS706 Standards Drafting Team ("the SDT") and commends the team for its work. While we have checked "Disagree" for many of comment boxes above, in each case we have attempted to provide constructive comments to improve upon the clarity and quality of the draft standard and where possible, to simplify the steps that registered entities must undertake to ensure both BES cyber-security and auditable compliance. APPA Task Force Comments: Independent 3rd Party Review The APPA Task Force is encouraged by the tiered approach to cyber-security proposed by the SDT, but is concerned that any bright-line metrics must be based on operationally sound regional parameters for BES planning and operations. We agree that use of entity-specific parameters concerning the classification of BES systems should be avoided, because this triggers the same difficult study issues that proved problematic during the identification of Critical Assets under CIP-002-1. However, while the need for entity-specific studies is reduced by using "bright line" regional metrics such as Contingency Reserves and IROLs that define normal and emergency operations, we cannot completely eliminate the need for entity-specific and sub-area studies. Many regional "fill-in-the-blank" standards raise similar issues. For example, the UFLS Standard Drafting Team, in its efforts to determine who should perform region-specific UFLS studies (e.g., to determine how much load to shed at what frequency and with what time delay), has considered a proposal to create a new Registered Entity called the "Regional Planning Coordinator Group." For these reasons, the APPA Task Force recommends that the CSO706 SDT propose to create a new Registered Entity called the "Regional Planning Coordinator Group." Similar in concept to a Reserve Sharing Group, all of the Planning Coordinators in a region would be required to become members of the Regional Planning Coordinator Group and would be required to perform and/or approve regional

Organization	Question 13 Comments (Response page 25)
	studies. The Regional Planning Coordinator Group would also be charged with the review and approval of studies by individual Registered Entities that propose to depart from the regional parameters and bright-line criteria approved under Attachment 1. The SDT should also describe the criteria that the Reliability Assurer will utilize to approve the assessment methods. Please note that the APPA Task Force understood "Reliability Assurer" to be a function performed by the Regional Entity. However, we are unclear how this functional responsibility can be distinguished from the Regional Entity's functional responsibility as the Compliance Enforcement Authority. The approach outlined above addresses regulatory directives that NERC standards not assign responsibility to comply with standards to the same entity that is responsible for assuring compliance with standards, while ensuring that the entity or entities responsible for performing regional studies have a wide-area perspective and the capability to fully assess the impacts of planning and operating studies. The Process for Industry Approval of CIP-002-4 Must be Synchronized with CIP-003-4 through CIP-009-4. We believe the industry the industry will find it difficult to reach consensus in support of CIP-002-4 and address all of the technical issues raised by this standard prior to its review of the associated security controls being developed standards CIP-003-4 through CIP-009-4. CIP-002 through CIP-009 cannot be taken one at a time. The APPA Task Force recommends that the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment. Under this revised development plan, the industry will have the opportunity to understand the whole suite of standards before they vote to give final approval to CIP-002-4. The APPA Task Force would support an industry-wide straw vote to garner conceptual approval of the next version of CIP-002-4 standard. Once so approved, the draft CIP-002-4 could be provided to the FERC and other regulatory bodies either on an informational basis or for conceptual approval. Such conceptual approval by industry and regulators would give the industry, the SDT, regulators and Congress greater confidence that NERC is making strides to complete this project expeditiously, while ensuring that the target end-state will be acceptable to stakeholders and government authorities. Responsibility for Jointly Owned and Operated BES Systems and Cyber Systems: CIP-002-4 should ensure that entities with joint ownership of BES Cyber Systems and associated Facilities coordinate their efforts to comply with the standard. Furthermore, CIP-002-4 should result in the identification of only one responsible entity for each BES Cyber System, and provide that only entities responsible for a BES Cyber System are required to comply with CIP-003-4 through CIP-009-4. Our reasoning is as follows: there are many cases in which multiple registered entities own a BES Facility, while only one of the co-owners owns and operates the associated BES Cyber System.
Consumers	Comment #1: Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in "version 3" to the approach in "version 4" is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be in scope. Comment #2: We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be

Organization	Question 13 Comments (Response page 25)
	interpreted to be in scope in version. Comment #3: We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable. Comment #4: Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. Comment #5: There are multiple alternatives for blackstart cranking paths. The standard needs to specify the “primary” cranking path. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the “primary” cranking path should not be considered as high or medium impact BES Subsystems. Comment #6: Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009 being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. We are not against this narrowing of the standard and believe that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. We have made a number of edits around this position and we hope that the SDT includes them in the next posting. We offer up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical) 1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment

Organization	Question 13 Comments (Response page 25)
	1 if they perform an engineering evaluation / assessment that satisfy Requirement 2. R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…” 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by

Organization	Question 13 Comments (Response page 25)
	the responsible entity. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) 2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (We Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entity are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit.

Organization	Question 13 Comments (Response page 25)
	1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: We removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? A transmission-only company would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or generation) We believe strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)

Organization	Question 13 Comments (Response page 25)
NPCC	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.” to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline
SWPA	The Applicability Section should be changed to delete Section 5 “Physical Facilities” and replace it with the language currently found in CIP-002-2, Applicability Sections 4.2.1 and 4.2.2 which state that facilities regulated by the NRC are exempt as well as those cyber assets (or BES cyber systems) associated with communication networks are exempt. The industry should not have to vote on CIP-002-4 prior to the development of the security controls which will apply to facilities or systems included in the scope of CIP-002-4. The standards that delineate the scope of facilities covered and the standards which delineate the security controls to be applied should be voted on as a package. If not, then the effective date of proposed CIP-002-4 should explicitly state that CIP-002-4 should be approved concomitantly with the effective dates of whichever standards are developed which apply security controls to this proposed standard. For the proposed definition of Cyber System: Is it up to each entity to determine whether underlying systems are a part of a given discrete system? Does each "Cyber System" necessarily consist of all its support systems? For the proposed definition of High BES Impact: Who performs the implied risk analyses? Will they be quantitative or a qualitative analyses? Who determines what level of risk is acceptable? How is this risk calculated? Who may accept residual risk? Who may authorize risk transferral? What risk analysis method will be used? In the field of Information Security, the word "risk" has a very specific meaning. If the full power to properly manage its risk is not granted to entities, another word should be used. The standard should contain a “no impact” category. Alternatively, any facilities included in the “low impact” category should not have security controls applied to them as they have no direct adverse impact to reliability. The industry should concentrate on those systems/facilities which potentially have a high impact to reliability. FERC Order 706 told NERC to consider the NIST framework. We strongly support that recommendation; the NIST 800 series allows flexibility in its implementation and acknowledges at its core that "one size fits all" cyber security approaches are doomed to failure. The NERC CIP standards are a compliance-based requirements framework; the NIST 800 series is risk based grounded in performance measurement and residual risk acceptance. The distinction is very important. Even though all traces of the word "risk" may have been scrubbed from the proposed CIP 002-4 draft, the fact will remain that cyber security is inherently all about risk management- it is impossible to remove the concept of risk management from an effective cyber security program. The more the CIPs evolve, the more they are beginning to resemble a reinvention of the NIST wheel. However, the most glaring departure from the NIST approach is demanding that there be zero leeway for entities to assume any risk whatsoever, yet at the same time placing the burden of securing the BES in its entirety upon each individual entity. The proposed CIP 002-4 draft uses a "high/medium/low impact" approach like FIPS-199, which is the document that provides security categorization guidance for the subsequent implementation of the NIST-800 series. The very fact that different levels of "impact" exist means that the unavailability of different systems has differing results on the Bulk Electric System. This is called risk categorization.

Organization	Question 13 Comments (Response page 25)
	NERC can rename it to anything they wish, but it is still risk categorization. In keeping with the NIST approach being grounded in performance measurement, the Version 4 CIP standards would be a good candidate for a proof-of-concept demonstration of NERC's results-based standards (Project 2010-06).
MPPA	Recommend tightening the definitions as well as ensuring that they are consistent with other non-cyber standards. MPPA is very concerned about having to approve standards foe the HML model, without know what compliance is required at each level. MPPA supports approval of the standards as a complete set.
Central Lincoln	Other Comments not already provided in response to earlier questions: We understand the other CIP standards will also be revised. We are somewhat in the dark in commenting, since we don't know how the categories will ultimately be used in the other standards. We hope that the ballot of CIP-002-4 will be concurrent with version 4 of the other CIP standards so that we will understand the full implications. We understand the SDT is attempting to write a standard that provides brighter line than the prior versions. The proposed revision does not yet hit that mark, but we are hopeful that industry comments will help in this regard. At the same time, we are concerned that the fast track this standard is on will shortcut the comments and the resolution of those comments yielding a standard that has dimmer lines than what is intended.
TransAlta	It is understandable that the draft team adopt high, medium, and low BES impact approach to categorize BES cyber system in order to "allow for requirements that are commensurate with the potential impact". But this can only be supportive in a condition that the cyber security controls to be drafted in the CIP-003 to CIP-009 would be properly assigned to the BES cyber systems based on their level of BES impacts.
NERC	1. It would appear appropriate to tie the effective date of CIP-002-4 to the regulatory approval of the remaining CIP Standards; 2. modify the Physical Facilities section to read "All BES facilities, (including those structures, systems, and components that are Balance of Plant "support systems" that do not adversely impact nuclear safety, security and emergency preparedness within a nuclear generation plant as defined by agreements between the ERO and the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission)." 3. The use of the opt-out engineering and assessment-based methods in Attachment 1 significantly dilute the objective bright-lines being sought, and leave the standard subject to fair criticism for being self-deterministic. Much clearer lines of delineation are needed and one way to accomplish this is to remove the engineering evaluation piece with the associated RC or Reliability Assurer oversight. This by itself would go a long way to keeping the lines clearer. 4. Applicability – if a Reserve Sharing Group has cyber assets that help it function, then it needs to be included in the list. 5. Measure M1 could be more direct: The Responsible Entity shall have a dated and categorized list of BES Subsystems as required by R1. 6. The approach is a significant improvement over the current standard. The standard is definitely heading in the right direction and we welcome the opportunity to support the team in accomplishing its objectives.
Dominion	In preparing these comments, Dominion has made assumptions that will likely be impacted by revisions to the content of standards CIP-

Organization	Question 13 Comments (Response page 25)
	003 through CIP-009 that are not yet available. Dominion suggests that once those revisions are available industry participants be provided with another opportunity to review and comment on this CIP-002 proposal. Generally, Dominion has concerns with removing the "routable protocol" language in the existing CIP-002 R3 standard. Entities have based current compliance activities on this language, and removing it significantly expands the scope of the standard to all cyber systems. It is unclear whether removing the "routable protocol" language will result in a corresponding improvement in BES reliability. Attachment 1, item 1.3 says - Each Generation Subsystem that has been pre-designated as Reliability "must run" units. Comment: As it pertains to this standard, Dominion disagrees with classifying Reliability "must run" units as high. In organized markets, such designation usually occurs only when a generator retirement is announced. When this occurs, organized markets have mechanisms to incent either the development of transmission or generation to allow the retirement of the generator as requested by the owner. This queue process is typically complete within 2-5 years, but it may take longer. Therefore, this designation is short term (2-5 years) in most cases. This short time frame may not allow the owner to implement the changes necessary to comply with the CIP standards before it would subsequently be allowed to retire. If this requirement is kept, Dominion suggests that it be modified so that the entity making the designation has a commensurate obligation to provide the term of such designation. In addition, the requirement should be further modified to allow the owner sufficient time to become compliant with CIP standards.
Encari	No
SCE	SCE believes that NERC should not conduct balloting on CIP-002-4 until the NERC Standards Drafting Team has prepared the revisions to CIP-003 through CIP-009. The categorization of the BES Cyber System cannot be properly conducted in a vacuum that does not consider the Security Controls that will be associated with the categories. We encourage NERC to accept FERC's advice that it is illogical for NERC to rush through CIP-002-4 when NERC has already been informed that NERC and the industry will have to await the completion of CIP-003 through CIP-009 before FERC will rule on the entire set of revised CIP Standards. We appreciate NERC's efforts to CIP-002-4 to date and believe that balloting the standard along with its accompanying suite of CIP standards would be ensure that NERC's efforts are most productive. Combining the voting periods for CIP-002-4 with the other CIP standards would also allow NERC to provide for a clear Implementation Plan for CIP-002-4. It is unclear how an implementation plan can be crafted in the absence of completed revisions to CIP-003 through CIP-009.
USBR	General Comments concerning the Standard: We believe the proposed changes will further complicate identification of critical cyber assets and place additional burden on the industry with little defined results. Furthermore, we are concerned with the proposed passage of a single standard without clear idea of what changes and modifications are going to be proposed for the remaining interconnected standards. We cannot agree to something when we do not know what the defined outcome or requirements are. It feels as if CIP-002-4 is being accomplished in a vacuum without a global understanding of the entire body of requirements. Recommended language adjustments for the SDT to consider:

Organization	Question 13 Comments (Response page 25)
	Definition Current Text: Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy. Recommended Change: Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and[inset"/or"] Control Center) used to generate energy, transport energy or ensure[delete "ensure"][insert "directly support"] the ability to generate or transport energy. Issue/Rationale: The use of the “and/or” language is more consistent with the remainder of the sentence. The use of the term “directly support” does not presuppose that the facility(ies) in question are essential. Definition Current Text: Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: Recommended Change: Control Center — A Control Center [delete "Control Center"][insert "centralized BES operations center that"] is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following: Issue/Rationale: Current language uses the same term it is attempting to define. Definition Current Text: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems Recommended Change: • Supervisory control of BES assets, including generation plants, transmission facilities, [insert "and"] substations [insert"/switchyards"]

Organization	Question 13 Comments (Response page 25)
	• Automatic Generation [insert "and Voltage"] Control systems or automatic load-shedding systems Issue/Rationale: Separate out individual Control Center functions rather than grouping in this manner. AGC and Load Shedding are not necessarily considered “Supervisory Control” as much as they are automated control systems (alternatively, define “supervisory control” from the perspective of automated controls.) Consider adding voltage or VAR control to the list. Requirement R1.1 Current Text: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change. Recommended Change: The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that could affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion [delete " completion"] [insert "effective in-service date"] of the change. Issue/Rationale: The Subsystem could be in-place and in-service for an extended period of time before it is considered “complete” or is even “commissioned.” We suggest the drafting team close the loophole. If the subsystem is complete enough to be in-service, it is complete enough to list. Requirement R1.2 Current Text: The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1. Recommended Change: The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the [insert "required"] categorization of BES Subsystems where required by [delete "where required by "][insert "as outlined in"] Attachment 1. Issue/Rationale: The language is unclear. It is not easily determined if an engineering evaluation is also a part of the work required under Attachment 1 Requirement R2

Organization	Question 13 Comments (Response page 25)
	Current Text: (Not cited) Recommended change: Add language indicating that information exchange with partners should be conducted in accordance with proper Critical Information Protection procedures. Sub-requirement R2.1 Current Text: Description of the Generation Subsystem that includes Facility designation(s), or name(s), location, and other identifiers needed to identify the Facility(ies) Recommended Change: Be more specific regarding “other identifiers.” Specifically, what information is required for each identified BES Subsystem? Requirement R3.1 Current Text: Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Recommended Change: Define “adversely impact” in terms of the BES. The terms used here and in Attachment 2 place no measures on what constitutes “adverse.” Consider defining “adverse” in real terms specific to the regional operating criteria. Violation Severity Levels For Requirement R2, Severe Current Text: The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its impact categorization for more than 90 days after the categorization. Recommended Change: The Responsible Entity has failed to notify its directly interconnected Transmission Subsystem owner(s) of its [delete "its"][insert "the"] impact [insert "categorization of its BES subsystems"] for more than 90 days after the [delete "categorization"][insert "date these Requirements become effective, or the effective service date of any new BES Subsystems, as appropriate"].

Organization	Question 13 Comments (Response page 25)
	Issue/Rationale: The language is unclear and readily misinterpreted. As written the language could result in NERC having no ability to penalize entities that simply never did a categorization of subsystems under this Standard (and therefore did not notify partners after they completed a categorization.)
Dyonyx	Great job by the Standards Drafting Team! In summarizing our comments, we believe more definition needs to be made to specific terms used in the draft document as delineated in our comments. In our opinion, every effort should be made to simplify the criteria and make it as objective as possible. In addition, where objective criteria can be used, there should not be any alternatives to use "engineering evaluation or other assessment methodology" to circumvent the specified criteria. For example, any Generation Subsystem "whose aggregate output exceeds the largest value of Contingency Reserve or total Reserve Sharing Obligations" should be absolute, i.e., no exceptions. The same applies to black start Generation Subsystems, cranking paths for Transmission Subsystems, etc. In consideration of the black start units and cranking paths, the restoration plans become quite relevant. More attention needs to be given to the issue of redundancies, multiple black start units and synchronization paths as they relate back to the categorization of BES Subsystems. Lastly, we are very concerned about the industry blessing these changes without having first understood the proposed requirements for the remainder of the standard. For example, how will the Cyber Security Controls be applied to Medium and Low Impact BES Cyber Systems? How will IP-based protocols be considered in the need to apply relevant Cyber Security Controls? While we understand the costs for implementing the standard in the eyes of FERC may not be a consideration, the industry needs to have a voice in establishing reasonableness such that the provisions of the standard can be met without bankrupting the underlying functional entities. After all, the functional entities have a responsibility for being "prudent" in protecting the rate payers while balancing the application of appropriate security provisions accordingly.
MISO	In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. We are also concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving

Organization	Question 13 Comments (Response page 25)
	to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA if it is also registered as the BA? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation. We are concerned about the addition of the function entity Reliability Assurer. While it was added to the most recent Functional Model, we believe it is premature to begin using this entity. While many believe that NERC and the Regional Entities are ultimately the Reliability Assurer, the function model is not clear this is the case. Furthermore, the Functional Model Working Group purposely drafting the Functional Model in a way so that it does not have to be the Regional Entities and/or NERC. Does the drafting team have a vision of whom the Reliability Assurer is? It has not been shared and we believe the drafting team needs to make clear whom they believe serves this role before it is added as new functional entity. Has this addition been coordinated with NERC certification and registry staff whom will have to register and certify this entity?
Westar	CIP-003 to 009 version 4 should be developed in parallel with CIP-002. They should be developed and voted on as a package.
Green Country	It is a widespread feeling that this standard no matter what its final draft ends up being should only go to vote as a package with CIP-002 thru CIP-009 since they are totally dependant on each other. Get this draft done, present 3-9 drafts for "informal" comment. Develop a final draft package and move on with them as a group.
Oregon PUC	The Safety Reliability Security Division of the Oregon Public Utility Commission appreciates the hard work of the SDT in the drafting of CIP-002-4. We also appreciate the many organizations that support the SDT team members and those that actively comment on this

Organization	Question 13 Comments (Response page 25)
	critical standard proposal. We strongly support NERC standards and requirements that bring sound value to the reliability of the electric grid. Standard CIP-002 is a cornerstone standard for which so many other NERC standards and requirements depend. This standard, even more critical than others, needs to be clear, specific and technically defensible. If we don't get this standard right – utilities, operators, and their ratepayers will suffer the cost of exposure to unending interpretations, corresponding enforcement actions, unnecessary diversion of resources and time away from more meaningful transmission investments. We apologize that we cannot give more meaningful comments at this time. We understand the impacts of CIP-002-4 are far-reaching to numerous other NERC standards, especially CIP-003 through 009. Our concern is that changes to CIP-003 through CIP-009 will have profound financial impacts to utilities and their ratepayers. Until the industry can understand these impacts in whole, we are skeptical of the benefits and costs. We would definitely recommend that the SDT do a benefit-cost analysis for the Low BES Impact Level taking into account probable changes to CIP-003 through CIP-009 standards. Likewise, the SDT should do a benefit-cost analysis for the Medium Level. Also, we recommend that a comprehensive implementation plan be developed for CIP-002-4 Medium and Low BES Impact levels. These levels should have delayed implementation schedules to allow time for compliance in concert with the changes in CIP 003 through 009. The risks associated with the lower levels are lesser so the urgency for prompt compliance is not as great as the high level. We also recommend that CIP-002-4 for the two lower levels be used as a trial-use guide until the next versions of CIP-003 through CIP-009 are approved by FERC. During the trial period, audits should be performed to determine how the CIP-002-4 is interpreted and enforced, but without sanctions.
Manitoba 1	no
Portland GE	Portland General Electric ("PGE") has been involved in NERC's Cyber Security efforts since Urgent Action 1200. PGE has identified critical assets for its Balancing Authority, Generation Owner/Operator, and Transmission Owner functions. While PGE appreciates the Standards Drafting Team ("SDT") considering changes to CIP-002 to address FERC Order No. 706 cyber security directed modifications and encouraging industry discussion, PGE has significant reservations about implementing these wholesale changes at this time. Registered entities have devoted significant resources to implement CIP compliance programs to meet the current requirements, and it is simply too soon to scrap those efforts and require entities to start over building new compliance programs to meet new CIP standards. While PGE would support certain improvements to the existing cyber security standards, PGE does not support the complete paradigm shift proposed by the SDT. The SDT has given very little reasoning for the scope of the proposed changes, and cannot justify requiring Registered Entities to start over on CIP compliance at a time when those entities are still building compliance programs to meet the current CIP requirements. To justify the entirely new approach to cyber security regulation proposed by the SDT, the SDT would have to build a record demonstrating the ineffectiveness of the current standards, and no such record exists at this time. To the extent the SDT believes the current standards to be insufficient to protect the reliability of the bulk electric system, the SDT should propose incremental improvements to the existing standards rather than prematurely changing course entirely. For example, if the SDT perceives that registered entities are under-reporting critical assets and/or critical cyber assets, the SDT should determine whether such under-reporting is the result of

Organization	Question 13 Comments (Response page 25)
	(1) a lack of clarity in the current requirements, or (2) an effort by Registered Entities to evade their CIP compliance obligations. If the SDT determines that the problem is a lack of clarity in the current CIP requirements, the SDT can clarify those requirements in a manner that should drive entities to designate additional critical assets and critical cyber assets. If the SDT determines that the under-reporting is an effort by registered entities to evade their compliance obligations, that problem would be best addressed through the compliance and enforcement process. Similarly, if the SDT desires to implement a risk management framework akin to the NIST Framework, that too could be accomplished through incremental modifications to the existing cyber security standards rather than by starting over with the approach proposed by the SDT. Prior to imposing requirements on systems and facilities that are not truly "critical" to the reliability of the bulk electric system, the SDT should seek information on how utilities currently protect those systems and facilities. For example, PGE, like most other companies, must follow good utility practice and have cyber-security policies in place to protect all of its cyber assets from just the threats that are contemplated in these standards. The SDT should gather information from entities and build a record supporting the need for moving toward something like the NIST Framework if the SDT believes that such a modification would enhance the reliability of the bulk electric system. While PGE does not support the scope of revisions proposed by the SDT, PGE also finds it difficult to comment on the specifics of the proposed standard without knowing this standard's effect on the current CIP-003 though CIP-009 standards. PGE and other ballot holders are unable to fully evaluate the framework established in CIP-002 without understanding the scope of controls that will be included in the standards that will succeed the current CIP-003 through CIP-009. With the current CIP-002 draft, PGE is unable to determine to what extent the Standards Drafting Team has drawn the lines between "High," "Medium," and "Low" BES Impact, and therefore the full regulatory impact of these categories is unknown. Additionally, this paradigm shift turns a clearly defined standard, which gives utilities the ability to build risk-based methodologies that work for their particular systems into a standard that is entirely subjective, with few defined terms. This causes great concern, most significantly for auditing and enforcement purposes. For example, "unacceptable risk" is an undefined term, and therefore subjective to each company – and to each auditor. Moreover, it appears that the CIP standards are being developed and revised in a "vacuum," rather than in conjunction with the bulk of the mandatory reliability standards ("Order 693 Standards"). This could create a "security versus reliability" issue for companies. Clearly, both security and reliability are important and the purpose behind the efforts of the regulators and utilities in implementing the mandatory NERC reliability standards regime. PGE believes there is some risk that the proposed standards could provide a disincentive to utilities to upgrade equipment to enhance communications and reliability because such upgrades could bring the equipment into scope for a higher level of CIP controls. Because they require an independent assessment of a utility's equipment from those studies already performed under the Order 693 Standards, these proposed CIP standards could set a different – and possibly higher – standard for reliability than the Order 693 Standards. For example, the Transmission Planning Standards ("TPL Standards") from Order 693 set specific circumstances and planning studies for transmission planning to maintain the reliability of the system. The CIP-002-4 standard as proposed creates an entirely separate regime under which the facilities are assessed. The utilities are then faced with the task of doing separate studies for the same facilities to achieve the same purpose – the reliability of the bulk electric system. The SDT should look to achieve efficiency and consistency between the two sets of standards where possible, and it appears that the proposed standard would, if

Organization	Question 13 Comments (Response page 25)
	anything, result in inconsistencies and inefficiencies. Finally, this standard as proposed would create great burden to utilities. Just as companies are finalizing their current CIP compliance programs and, in PGE's case, preparing for its first spot check of its CIP compliance efforts, they are being asked to weigh in on a completely new approach to CIP compliance. For example, all documentation identifying critical assets or critical cyber assets would require material changes, and the proposed standard would exponentially increase the number of assets considered to have an impact on the bulk electric system, many of which have no communications abilities or any actual potential impact on the reliability of the system. The tracking and reporting requirements included in this standard are not only burdensome, but would also create a substantially higher compliance risk to utilities without necessarily enhancing reliability. PGE recommends that NERC wait until the results of the initial round of spot checks are analyzed before taking such a drastic step to overturn the current regulatory framework. PGE also encourages the SDT to consider the potential compliance risk inherent in such a fundamental change to existing cyber security controls. Companies, including PGE, have invested a great deal of money and the efforts of a large number of employees into establishing compliance with the current standards. Companies including PGE have invested a great deal of money and the efforts of a large number of employees into coming into compliance with the standards as they are written. PGE has spent thousands of hours identifying its critical assets and associated critical cyber assets and developing compliance programs, procedures, and documentation to demonstrate compliance with the current CIP standards. Under the proposed standards, all of the work identifying critical assets and critical cyber assets would be effectively scrapped, and all of the compliance programs, procedures, and documentation would, at a minimum, require substantial changes. The SDT should consider the very real possibility that some individuals and entities will discount the importance of their future CIP compliance efforts if their efforts to date are written off at this early stage in favor of a new regulatory paradigm. A wholesale paradigm shift to these regulations, especially one that is not clearly written and objectively defined, will lead to confusion on the part of the front-line employees responsible for complying with these regulations. Constant changes to the controls under which people perform their day-to-day tasks could potentially create general uncertainty about which controls are in place and what an employee's obligations are at a given time. The risks of such constant changes to the cyber security regulatory scheme should be taken into account when contemplating a change of this magnitude. Instead of changing courses entirely, the SDT should value the thousands of hours and millions of dollars of CIP compliance work that has been done under the current standards, and work to improve the reliability of the Bulk Electric System through improvements to the existing CIP standards.
PSEG	Comment #1: Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in "version 3" to the approach in "version 4" is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be in scope. Comment #2: We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be interpreted to be in scope in version. This stepping block could be structured as per comment #3, following. Comment #3: We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE

Organization	Question 13 Comments (Response page 25)
	applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable Comment #4: Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. Comment #5: There are multiple alternatives for blackstart cranking paths. The standard needs to specify the "primary" cranking path for initial system restoration. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the "primary" cranking path should not be considered as high or medium impact BES Subsystems. Comment #6: Those companies that have made a significant investment in designing Blackstart plans, including multiple cranking paths and blackstart units affording great flexibility and redundancy, should not be effectively punished for having a diverse set of assets available for system restoration. Only primary units and cranking paths used for initial system restoration should be considered as high or medium impact BES subsystems. Comment #7: Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009 being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. We are not against this narrowing of the standard and believe that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. We have made a number of edits around this position and we hope that the SDT includes them in the next posting. We offer up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical) 1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment 1 if they perform an engineering evaluation / assessment that satisfy Requirement 2.

Organization	Question 13 Comments (Response page 25)
	R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its ownership by applying the criteria in CIP-002-Attachment 1…” 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by the responsible entity.

Organization	Question 13 Comments (Response page 25)
	(Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) 2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Comments on Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (We Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entities are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.2 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.3 Each Generation Subsystem that has been pre-designated as Reliability "must run" unit. 1.4 Each Transmission Subsystem which contains Facilities that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher

Organization	Question 13 Comments (Response page 25)
	in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.5 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.6 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.7 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.8 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: We removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? A transmission-only company would not know how to apply the 2,000 MW level. (Does this apply to the MW's of load or generation) We believe strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.1 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.2 Each Transmission Subsystem which contains Facilities that are operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection. Restoration Criteria: 1. Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit has high. 2. Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.) 3. Entities that have a multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard. 4. Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)
WE-Energies	Wisconsin Electric Power Company contributed to and supports EEI's comments regarding this question. Wisconsin Electric Power

Organization	Question 13 Comments (Response page 25)
	Company also agrees with comments as put forth by Midwest ISO. In addition Wisconsin Electric Power Company has the following comments: • Two year implementation is too short. A compliance infrastructure did not exist for the generation entities as it did for BA entities, and should allow additional time for compliance activities. • Need to better define the term "under its ownership". Does this include telecommunications systems (telephones)? • The definition of Cyber System does not include the category of control. We further recommend more clarity in the list of attributes. For example, what does "maintenance" apply to? It should not include test equipment and data. • Under High BES Impact, use the NERC Glossary term “Cascading”. Also, the term "planning time frame" is not clearly defined. Does this mean we have to make a new assessment for every unit outage and line outage? Recommend removing the language around the planning time frame. • Physical Facilities uses the expression BES facilities and then further expounds by listing "those structures components, equipment and systems of facilities within a nuclear generation plant ...). We're not sure if the intent is to use the NERC Glossary term Facilities which is already defined, or if this is intended to be "facilities." • CIP-002-4 effective date should coordinate with the CIP-003 through CIP-009 V4 effective date. • It is difficult to agree with the direction taken by this standard without examining the impact of how the compliance standards CIP 003- CIP 009 would apply to these asset categories. Wisconsin Electric Power Company recommends a more evolutionary approach which would keep the current CIP-002-2 critical asset and associated critical cyber asset determination and methodology, but enhance it by using the proposed attachment 1 high and medium impact criteria for critical asset determination. • The category Low BES Impact should be dropped - too inclusive. Per the definition, low impact assets have little or no effect on BES reliability. • It is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use “legacy serial” communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means.
Idaho Power	This draft is a drastic change from previous versions and will require sizable effort from the Registered Entities to comply with proposed changes. A realistic implementation schedule along with comprehensive guidance/assistance is essential to Registered Entities to successfully implement the proposed changes. It would also be helpful to get some idea about what CIP-003-009-4 will look like before gaining approval of CIP-002-4. Compliance with the CIP standards is costly and expanding the scope of CIP in this proposal will make it even more so. Although cost is not an excuse for non-compliance, it is a factor for most entities that requires that we plan and budget for well in advance of a compliant date. We support the position that the categorization of the cyber systems by their impact on critical BES functions is a more straight forward approach and relieves the entities of the burden to categorize all of their BES subsystems. A fairly comprehensive list of the cyber

Organization	Question 13 Comments (Response page 25)
	systems that should be considered in the categorization process would be very helpful.
SOCO	Explicit provision should be made for joint ownership of a BES subsystem. The 8 quarter implementation deadline from the date CIP-002-4 is approved is concerning because version 4 of CIP-003 thru 009 will most likely not be finalized and approved until six months after CIP-002-4 is approved. We cannot make implementation plans or actually implement cyber and physical controls at newly identified cyber assets that result from CIP-002-4 without knowing what the required controls will be for the high, medium, and low impact categories. CIP-002-4 is going to significantly increase the in-scope cyber assets associated with Transmission Subsystem assets. We recommend that the 8 quarter implementation deadline start from the point version 4 is approved for all of the CIP standards (CIP-002 thru 009). This comment has already been made and the Substation representatives would like to restate it here. Unless there are no requirements at all for cyber systems associated with Low BES Impact Subsystems, requirements are being created for equipment which carry no risk to the BES. Either all Low BES Impact Subsystems should be exempt from the CIP-003 through CIP-009 standards or a category for minimal-risk or no-risk subsystems must be created. Voting on CIP-002 apart from being able to see the actual controls required per category is asking the industry to put themselves in the difficult position of determining if the scope and classification is correct before we know anything about what each classification means in terms of security requirements. Breaking the set of standards up and sending CIP-002 to FERC ahead of the other requirements has been unfairly imposed on the drafting team. Lack of 'Bright Lines'. The industry wants ‘bright lines’ in the standard so that compliance state is objectively deterministic and not subject to interpretation in audits. There are two areas where bright lines are still not evident: 1. Defining BES Subsystems. Even though Attachment 1 is striving to provide bright lines for classifying BES Subsystems, there are few to no rules for determining what a BES Subsystem is. An entity and the regulator could define them totally different for any given asset such as a plant. The drafting team itself has gone through exercises with simple plant diagrams and has had numerous conflicting answers on the resulting BES Subsystems in that plant. 2. Defining BES Cyber Systems. The current R3 has almost no lines at all and it’s the crucial one for a cyber standard. It simply asks for a list of cyber systems that can affect any of 9 Reliability functions (with 63 subfunctions listed) in Attachment 2. Pick “Situational Awareness”; what is the bright line that tells an entity or an auditor whether something is or is not part of situational awareness and should be on the list and how does either prove that you have them all? You could make the case that any and every cyber system is part of situational awareness. Next pick the “Control and Operation” function and consider how to provide evidence that you have every cyber system with any involvement in that on the list. Classification updates. The classification of all BES Subsystems and all BES Cyber Systems is a monumental task. The drafting team is attempting not to have that be a regularly occurring (annual) process but rather do it once and then maintain it as the BES assets and the cyber systems change. However, documenting 'changes in the electric system' and all subsequent classifications for compliance tracking purposes is problematic.
DTE	We think that a tiered approach is a more appropriate way to identify assets than the current Standards, and is also being utilized in other Homeland Security applications/regulations. (CFATS - Chemical Facility Terrorism Standards, MTSA with TWIC readers - Maritime

Organization	Question 13 Comments (Response page 25)
	Transportation Security Act & Transportation Worker Identification Credentials proposed rule, etc.) However, we prefer the criteria for asset identification at the various impact levels be established at the same time as the security controls/measures (cyber & physical) that are to be utilized at each level. It is not clear how this will affect CA/CCAs that have already been identified. We are concerned that entities have wasted time, money and manpower. There needs to be guidance on how to leverage work that has been done to protect CCAs in compliance with the current version of CIP. We recommend considering other physical security regulations for facilities that already have existing Facility Security Plans under (CFATS, MTSA, etc.) to eliminate duplication for entities having to comply with multiple regulations. We are concerned on how this change to the standard will affect an organization that may be audited partially under the old standards and partially under the new standards. Editorial Comment: Section A5 Physical Facilities should be under section 4 Applicability so Physical Facilities should be 4.2 and paragraph 5.1 should be numbered 4.2.1. Effective date then becomes number 5.
AEP	No additional comments at this time.
NS&T	We commend the SDT for the time and effort invested in developing the draft standard, and we thank the members for this opportunity to share what we hope are useful comments.
Flathead	I appreciate the efforts of the drafting team to respond to forces beyond their control. In general, this approach comes too close to regulating local distribution assets often not included in registration criteria, drawing staff and resources away from protecting what is truly critical. Encourage the team to limit this rewrite things that meet the medium and high categories.
E ON	Other Comments not already provided in response to earlier questions: E ON U.S. is concerned that CIP-002-4 draft is being proposed “in a vacuum,” without context of the requirements from the other CIP standards. It is one thing to categorize assets as high, medium, or low potential impact, but the real cost in compliance is in the protective measures that need to be implemented in response to this identification and rating of these assets. The cart may have been placed ahead of the horse. More information concerning how high, medium and low impact assets are to be protected is required before industry can reasonably be expected to sign off on CIP-002 V4. The methodology also seems to address cyber risks in a silo, without an overall risk-assessment of other threats against critical assets that should be considered for proper prioritization and investment in protective measures. It seems that some consideration should be given regarding cost/benefit analysis in meeting a control objective versus the value of the asset that is the target of protection. Future installation of programmable devices intended to enhance BES reliability will be weighed against the cost of complying with the Version 4 CIP standard requirements applicable to such devices. Entities may in fact disconnect existing systems. This may well result in decreased BES reliability. The drafting team appears to presume that the BES as whole, i.e., the BPS grid, the target of protection whenever CIP requirements are

Organization	Question 13 Comments (Response page 25)
	mandated for any size facility or associated cyber asset. This can only be true if industry is abandoning not only N-1 analysis but also any realistic attempt at examining reasonable contingencies. The standard appears to assume all of an entity's assets can be simultaneously compromised. The costs that are certain to result from this assumption demand that the assumption be challenged and debated not only by registered entities but by regulators at all levels responsible for protecting utility ratepayers.
Carthage	Please clarify All BES Facilities in section 5.1 of the standard. Is this intended to mean the facilities operated at 100 kV and above as the BES definition states? CWEP feels that there should be a category for No BES Impact as stated in number 8 above. CWEP feels that the CIP-002 thru CIP-009 Version 4 standards should be approved as a package so entities have a chance to review the requirements of CIP-003 thru CIP-009 before CIP-002 is implemented. The effective date of CIP-002 thru CIP-009 should be the same. CWEP feels that there should not be any mandatory controls for facilities that are low impact and have no communications. Again CWEP is okay with the format of the standard but would like for the criteria to be more specific. CWEP feels that applicability needs to be clarified throughout the standard to ensure that it's interpreted correctly as stated in numbers 8 and 12 above. CWEP feels that this could help eliminate any unnecessary confusion. The standard is very confusing as to whether it is intended to apply to smaller entities. Smaller entities being systems that operate at less than 100 kV. CWEP feels that the standard, as written, has the potential to place a considerable burden on smaller entities and not achieve much in the way of reliability. CWEP would like to request that clearer lines be established so that entities understand if the criteria applies to them or not.
WECC	We feel that attempts to limit analysis to only an impact based analysis has left things dependent on engineering study's and makes it actually more difficult to determine criticality. We feel that moving to a high, low, and medium impact is best done by bringing probability of an event back into the criteria. We do not agree with NERCs intent to remove probability from the risk assessment process, particularly with the return to classifying assets as high, medium and low risk.
Entergy	Comments and Recommendations Concerning Draft CIP-002-4 • Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective. • The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. • Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised.

Organization	Question 13 Comments (Response page 25)
	• CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. • The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… • The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below. Validity of the "Cyber First" Approach to Defining Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – system stability is the salient issue. • N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a coordinated multi-site attack, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on a perpetrator's ability to navigate across and between control system data networks in order to access multiple sites. • "Routable protocol" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented). • Thus, routable protocol networks are the correct object of cyber protection concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.] • At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means. • CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for all control system cyber assets that communicate in common on a TCP/IP-based data network infrastructure; regardless of how big or small the grid operating site is in terms of electrical rating. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities relevant in practice to BES reliability. • If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is not for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not

Organization	Question 13 Comments (Response page 25)
	be imposed where cyber threat is not real. • Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the different Categories of cyber assets as characterized below. Identifying Specific Cyber Objects of Protection • Start by identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement, execute, or support the Essential Functions. • Generally speaking, process and distributed control system elements at work at different types of grid operating site present three major cyber asset categories in terms of cyber risk exposure to the bulk electric system: o o Category 1 (High): Control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate; these require the most rigorous cyber security controls and countermeasures because nefarious root capture of control system hosts represents the worst case scenario. o o Category 2 (Medium): "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use. Dial-up aside herein, these cyber assets require earnest cyber security controls and countermeasures, but nefarious root capture of same typically does not directly represent the same grid threat severity as do control system host computers themselves. o o Category 3 (Low): Cyber assets in use at all other operating sites that do not employ routable TCP/IP protocols to communicate. These should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc). • Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset identified above. More granular refinement of cyber security control and countermeasure Requirements will be necessary beyond the gross categorical illustration above, especially concerning Category 2. • Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not in terms of facility size/rating] • All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I. Advantages of the Recommended Approach • It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The subject is computers, not electricity. • This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's

Organization	Question 13 Comments (Response page 25)
	complimentary improvement, not do-over. • It results in application of cyber defenses appropriate to true risk, and does not require expense and effort securing assets that do not pose a genuine vulnerability/threat. • It provides Responsible Entities the autonomy to manage gradual replacement of antiquated data networking in favor of high performance TCP/IP networking that demands more rigorous cyber security controls and countermeasures. • It buys the industry time to appreciate the impact of Smart Grid and NASPI on security controls/countermeasures needs prior to upgrading control systems networking.
CenterPoint	The proposed security control measures for CIP-003 – CIP-009 and overall implementation plan for Version 4 should be provided prior to voting on CIP-002.
LCRA	Question - 8. D. Compliance, 1.3, bullet 1 – Does the phrase “last update” include the annual review? If the document is reviewed each year but not changed, is there a requirement to keep all old copies or just the most recently reviewed copy?
FRCC	In Section D, Compliance, Item 1.1.1 is not clear to me. I believe the drafting team is trying to say that if a Regional Entity is registered for a specific function, such as RC etc, then the Regional Entity can not monitor themselves. If not, I am confused with the use of the term Responsible Entities. For instance, the FRCC is registered as a Reliability Coordinator. The FRCC Compliance Staff does NOT monitor the FRCC RC as identified in the delegation agreement. But, the FRCC RC function does utilize an entity as an agent to perform the RC function. The FRCC Compliance Staff does, and should be able to monitor that particular entity for their own registered functions that are separate and apart from the function that they perform as the agent for the FRCC RC. And, 1.1.2 states that the ERO is the monitor for a Regional Entity. That does not have to be the case. FERC through the delegation agreements has allowed for other 3rd parties to be the monitor for a RE. I would suggest that this Compliance Enforcement Authority section just be revised to state that it would be per the ERO Rules of Procedure and the NERC/Regional Entity Delegation Agreements. The Reliability Standard should not dictate something that may be in opposition to what FERC or other governmental authority has allowed.
NIPSCO	Version 4 represents an enormous departure from previous versions. While the new version may be in line with the direction received from FERC, the transition from the approach in “version 3” to the approach in “version 4” is likely to be confusing and result in plentiful new interpretation-type questions. We are concerned about the level of cyber assets that could now be interpreted to be in scope. We believe that there should be a stepping block between what is currently in scope in CIP version 3 and what could be interpreted to be in scope in version 4. We suggest that a new intermediate version 4 simply take the existing version 3 and modify CIP-002-3 R1.2 to include some of the specific items in the draft CIP-002-4 attachment 1 document. This approach would result in a new version 4 with an expanded Critical Asset scope, a new implementation plan, and would act as a step between V3 and the proposed V4. We also believe that this stepping block approach should address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories, inconsistencies in TFE applicability within a given requirement and that this new version 4 should

Organization	Question 13 Comments (Response page 25)
	include language addressing the final approved interpretations (RFI's) from previous versions.
ConEd	The associated Guideline on page 10 of the document states: "In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems." The Guideline provides an example for the SCADA system that causes the Control Center High rating to overshadow the other subsystems. It is not clear whether or not the SCADA (which would be a HIGH) would become so due to its control of all BES substations and generation plants through the station RTU devices cause all these "associated" subsystems to become HIGH by inheritance, or not. The intent of this requirement may have significant impact to our classification criteria if the SCADA causes other system to become rated HIGH • Attachment 1, item 1.5: what does "transmission lines leaving the station" mean? Suggest saying "transmission lines connected to the station". • Attachment 1, item 1.1: 'exclusion' does not make sense - if a generating plant is determined to "not be essential to the reliability of the BES", then why does it default to Medium? If the plant is not essential, it should either be categorized Low or excluded. Same comment applies to 1.5. • Attachment 1, item 1.2: Change "output" to MVA nameplate rating. Add "in the relevant RC region" to the end of the sentence. • Attachment 1, item 1.5: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 1.5: last sentence is missing the ending that appears in 1.1: "...in which case such Subsystems may be categorized as Medium BES Impact." • Attachment 1, item 1.10 and 1.11: this language seems to imply that each and every combination of substation needs to be evaluated to determine if the loss of that aggregate subsystem would have on frequency and voltage. Is this the drafting team's intent? • If Transmission Subsystem consists of one or more elements, how does an entity demonstrate to an auditor that all combinations of transmission subsystems were evaluated? For example if an entity owns 20 345 kV substations, do you have to evaluate every combination of the 20 as a separate subsystem? • Attachment 1, item 2.2: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 2.2: replace "they" in 4th line with "the Transmission Subsystem"

Organization	Question 13 Comments (Response page 25)
	• Attachment 2, Dynamic Response: spell out the word “Transformer”. Do not use abbreviation x-former. • Attachment 2, Managing Constraints is missing the word "function" in the second paragraph. R3.1: Each Responsible Entity shall list each BES Cyber System (associated with a BES Subsystem categorized in Requirement R1) that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Need to clarify that the "that" in R3.1 refers to BES Cyber System and not to BES Subsystem, perhaps by including the parenthesis added above. The Drafting Team has developed a “bright line” approach for categorizing BES Subsystems. In lieu of this approach, the Drafting Team is encouraged to consider use of an impact-based methodology, reviewed and approved by the Reliability Assurer, such as the NPCC A-10 Criteria. The Drafting Team should consider an “NA” (“Not Applicable”) designation for elements that fit the BES definition, but have NO impact on Interconnected Bulk Electric System. This designation would be "below" an even LOW impact level, allowing Entities to reflect the accurate impact/status of some of its system.
EEI	1. EEI supports NERC’s efforts to develop a complete revised set of CIP standards in 2010, with a plan to file the new set of Standards with FERC in early 2011. EEI and its members recognized the importance of this activity and are committed to this effort. EEI believes that the new CIP standards development project is one of the most important activities facing both NERC and the industry in 2010. 2. EEI believes that NERC can put forward a single package that includes both the proposed standard for BES Cyber System Categorization, as well as the associated controls. This will allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of associated controls. 3. EEI agrees that there is value in identifying clear and straight forward bright line criteria for high, medium, and low impact BES assets. The bright line criteria should be subject to an approved engineering evaluation in the event that an entity owns or operates an asset that while meeting certain criteria, does not affect the BES to the level indicated by the bright line. 4. EEI believes that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility exceptions (TFEs). 5. EEI believes that the current written definitions for high, and medium impact BES systems do not bring sufficient clarity for determining the appropriate category. EEI recommends using only the criteria identified in Appendix 1 to make such determinations. 6. EEI suggests that the drafting team use terms and definitions that exist within the NERC Glossary whenever possible, and avoid the use of vague language that may lead to subjective interpretation. 7. EEI believes that this SDT needs to be very clear that this standard can only apply to those facilities that are covered under FPA 215 as defined by the definition of BES. 8. Moving into the future,

Organization	Question 13 Comments (Response page 25)
	a. EEI believes that standards development team should focus on the "What" of security control outcomes rather than the "How". b. EEI suggests that the drafting team carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
O&R	The associated Guideline on page 10 of the document states: "In the case where a BES Cyber System supports multiple BES Subsystems, then the BES Subsystem with the highest impact categorization is inherited. Table 2: Example Impact Categorization for a SCADA System demonstrates this concept for an example SCADA Cyber System associated with multiple BES Subsystems." The Guideline provides an example for the SCADA system that causes the Control Center High rating to overshadow the other subsystems. It is not clear whether or not the XA21 SCADA (which would be a HIGH) would become so due to its control of all BES substations and generation plants through the station RTU devices cause all these "associated" subsystems to become HIGH by inheritance, or not. The intent of this requirement may have significant impact to our classification criteria if the SCADA causes other system to become rated HIGH • Attachment 1, item 1.5: what does "transmission lines leaving the station" mean? Suggest saying "transmission lines connected to the station". • Attachment 1, item 1.1: 'exclusion' does not make sense - if a generating plant is determined to "not be essential to the reliability of the BES", then why does it default to Medium? If the plant is not essential, it should either be categorized Low or excluded. Same comment applies to 1.5. • Attachment 1, item 1.2: Change "output" to MVA nameplate rating. Add "in the relevant RC region" to the end of the sentence. • Attachment 1, item 1.5: Change beginning of the item to read "Each Transmission Subsystem that contains one or more substation operated at……" • Attachment 1, item 1.5: last sentence is missing the ending that appears in 1.1: "...in which case such Subsystems may be categorized as Medium BES Impact." • Attachment 1, item 1.10 and 1.11: this language seems to imply that each and every combination of substation needs to be evaluated to determine if the loss of that aggregate subsystem would have on frequency and voltage. Is this the drafting team's intent? • If Transmission Subsystem consists of one or more elements, how does an entity demonstrate to an auditor that all combinations of transmission subsystems were evaluated? For example if an entity owns 20 345 kV substations, do you have to evaluate every combination of the 20 as a separate subsystem? • Attachment 1, item 2.2: Change beginning of the item to read "Each Transmission Subsystem that contains one or more

Organization	Question 13 Comments (Response page 25)
	substation operated at……" • Attachment 1, item 2.2: replace "they" in 4th line with "the Transmission Subsystem" • Attachment 2, Dynamic Response: spell out the word “Transformer”. Do not use abbreviation x-former. • Attachment 2, Managing Constraints is missing the word "function" in the second paragraph. R3.1: Each Responsible Entity shall list each BES Cyber System (associated with a BES Subsystem categorized in Requirement R1) that has the potential to adversely impact any of the functions identified in CIP-002 — Attachment 2 — Functions Critical to the Reliable Operation of the Bulk Electric System. Need to clarify that the "that" in R3.1 refers to BES Cyber System and not to BES Subsystem, perhaps by including the parenthesis added above. The Drafting Team has developed a “bright line” approach for categorizing BES Subsystems. In lieu of this approach, the Drafting Team is encouraged to consider use of an impact-based methodology, reviewed and approved by the Reliability Assurer, such as the NPCC A-10 Criteria.
Alliant	It is imperative that the rest of the CIP standards be developed before CIP-002 is balloted. We can not make an informed affirmative vote on this standard until we know what the controls will be for "High", "Medium", and "Low" impacts. There must be a "Not Applicable" selection of Impact as well. There are some cyber assets that have no impact on the BES, and that must be recognized. We believe there should be more clarity for what constitutes a cyber attack. The Standard needs to further clarify if it is protecting against singular or wide-spread attacks, or both.
Ameren	This current draft does not address the FERC concern of the industry being prepared to respond to "coordinated attacks”. It just appears to provide for a more consistent application of the current standard only. There needs to be a matrix approach to develop a list of high impact BES Subsystems that have high impact BES Cyber Systems required to be protected. How would protecting a low impact BES Cyber System in a high impact BES Subsystem improve the reliability of the BES, for example protecting a BES Cyber System that does not use TCP/IP or dialup accessible? There is no wording in this draft addressing the subject of “misuse” as dictated in FERC Order 706. It is hard to evaluate this standard without seeing the remaining CIP standards, CIP-003 through CIP-009 for security controls. Terms used in this draft of CIP-002 that are not defined in the NERC Glossary of Terms need to be added. For example; “Regional Reliability Assurer”, “adversely impact”, “unacceptable risk”, “instability”, and “shared element” Remove the definitions of High, Medium, and Low BES Impact in this standard and use only Attachment 1 for these definitions. Clarify how to utilize attachment 2 or add more criteria for defining BES Cyber System that have the potential to adversely impact any of the functions identified in CIP-002 Attachment 2. For example what about BES Cyber Systems that are not dialup accessible or do not

Organization	Question 13 Comments (Response page 25)
	use a routable protocol. How do these systems have the potential to adversely impact any of the functions in Attachment 2 if they are not remotely accessible? There needs to be definition of what is an acceptable engineering assessment that can be used to determine the BES impact categorization.
Black Hills	Concern that rigorous implementation of CIP-002-4 as currently described would dramatically increase the amount of BES sensitive information that would be shared among entities and consultants, which increases the possibility of that information being compromised or abused.
TNMP	TNMP has concern regarding retirement of the definition of "Cyber Assets." TNMP cannot envision how future versions of CIP-003 through CIP-009 will be applied with just the BES Cyber System definition. If the drafting team is preparing a paradigm shift permitting devices within an ESP but not part of a Cyber System to be exempted from CIP requirements, then the definition is not necessary. However, if the goal is to continue CIP protection of all Cyber Assets within an ESP containing a BES Cyber System, then the definition must be kept. If the term Cyber Asset is to be kept then TNMP would like a revision to the definition removing the phrase "and data."
NVEnergy	We commend the drafting team on their work thus far. This draft represents sweeping changes and paradigm shifts in the way critical infrastructure protection is to be handled. The draft revisions are heading in the right direction; i.e., applying a varying degree of security objectives upon those systems that have the highest degree of impact; however, the standard should focus on those accessible (routable protocol, IP, dial-up) cyber systems that have impact upon the reliable operation of the BES. Critical Assets, Critical Cyber Assets and Cyber Assets are terms that would be retired from the Reliability Standards Glossary of Terms. As such, upon implementation of CIP-002-4, all other CIP Standards (CIP-003 - CIP-009) would become defunct and/or unenforceable. The CIP-003 - CIP-009 Standards rely on the definition of Critical Assets, Critical Cyber Assets and Cyber Assets to define what needs to be protected, the level of protection required, the required security management controls, training and review, establishment of electronic security perimeters, physical and system security requirements, etc. CIP-002-4 does not provide the appropriate link from CIP-002-4 to the other Standards. The question of what an entity is to do after this categorization is left to be answered, and until the stakeholders can see the entire scope of the CIP version 4 re-write, it is difficult, if not impossible, to pass judgment on this CIP-002-4 in isolation.
MWDSC	Recommend delaying effective date or concurrently developing CIP-003 through CIP-009 in order to determine if CIP-002 is reasonable. Also needs more implementation time or readiness assessments before making mandatory. Vague or unclear terms create opportunities for differing interpretations.
Empire	Consider: 1. Routable protocol or dial up accessibility as a criteria 2. A category for NO impact to the BES 3. Low impact with no communications = no controls 4. Evaluate events based on a single contingency 5. Readiness audits prior to mandatory dates

Organization	Question 13 Comments (Response page 25)
	6. Financial impact vs. true BES impact prevention benefits 7. Approve CIP-002 though CIP-009 Version 4 as a package at the same time 8. Effective dates of CIP-002 same as CIP-003 through CIP-009 9. Performance based requirements 10. No ambiguous language
BCTC	The guidance provides a process overview to an organization to do a risk assessment on assets and could better serve utilities on how to actually walk through a CCA process identification using the functional requirements listed in CIP002. Closer tying it back to CIP-002 would be of more value. An abbreviated start/example, from a Control Centre perspective, using a functionality approach, building off of CIP-002-4 is detailed below. *** To begin, each utility should determine, based on their registration status, which critical cyber asset functionality described in NERC CIP-002-1 R3.0 is applicable to them. For a control centre, critical operational functionality includes: Monitoring and control – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable supervisory control and data acquisition function (e.g. monitoring and control) of remote assets that support the reliable operation of the BES; Remedial Action Scheme – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the arming of the Remedial Action Scheme; Automatic Generation Control – the information system(s)/applications(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the automated functionality to support Automatic Generation Control; Real-time Power System Modeling – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, and network infrastructure), that enable the modeling to enable the reliable operation of the BES; and, Real-time Inter-Utility Data Exchange – the information system(s)/application(s), and supporting cyber assets (e.g. servers, workstations, network infrastructure), that enable reliable information transfer between neighboring utilities required to maintain the reliable operation of the BES To be considered a critical cyber asset the cyber asset must: 1. Be a system/application deployed in a real-time Production Environment; 2. The system/application must meet on or more of the following section criterion: a. Enable remote Monitoring and Control functionality (e.g. SCADA); b. Enable Remedial Action Scheme;

Organization	Question 13 Comments (Response page 25)
	c. Enable Automatic Generation Control; d. Enable Real-time Power System Modeling; and, e. Enable Real-time Inter Utility Data Exchange. 3. The system/application must use a routable protocol (e.g. Internet Protocol) to communicate between discrete electronic perimeters; or, the system/application must have a direct dial-up connection to a public network (e.g. Plain Old Telephone Line). From this point, the utility could develop the cyber systems inventory, as suggested in the drafts “step 1 & 2”, and verify if the systems enable the functional areas using a matrix
SWTC	Attachment 1 addresses the need to ensure that studies have been done, and can be documented to show, with approval by the Reliability Coordinator, that if a transmission subsystem is destroyed, degraded or rendered unavailable, it does not need impact the BES. (This is an oversimplification of what is stated; both planning and operations studies will be needed to document this.) There is similar wording for generation subsystems. The proposed CIP standard gives a definition for "Cyber Systems" and "BES Cyber Systems" but provides no guidance as to what those are or how they shall be designated by transmission and generator owners and operators. Instead, the standard launches into requirements for BES Subsystems. Neither does Attachment 1 address these. However, it could be construed that Attachment 2 addresses these as it discusses functions critical to the reliable operation of the BES and outlines aspects of control-type systems that utilize protection systems and relays. Attachment 1: How does this apply to a small(er) utility? and Who does it apply to? Additionally, I agree with the idea of subsystems is an unneeded step and adds confusion. However, I think one positive to the standard, is that the terms "critical assets," "critical cyber assets," and "cyber assets," go away. The standard offers no impact or applicability tier to BES elements/subsystems that are not critical to the BES. In other words, we don't have to worry about our assets being designated as "critical," but the onus is on us to determine, through discussion, evaluation and study, if they have an impact to the BES.
SCEG	It is imperative that the SDT provide guidance to the entities on the Security Controls (CIP-003-009) that will result from the 3 impact classification levels. It is unacceptable to ask the industry to vote to approve a standard without knowing the implications resulting from the standards directly associated with it. If some guidance on the resulting security controls coinciding with the classification level were provided, entities may feel more inclined to approve the standard.
Exelon	Exelon appreciates the effort of the SDT and recognizes the task assigned to the SDT is extremely difficult and challenging. As the SDT stated in the cover letter the revisions to CIP-002 will impact the entire suite of CIP standards that are currently in force, all without a clearly stated scope of applicability from the USNRC to U.S. nuclear plant generator owners/operators. Providing salient comments only on CIP-002 revision without understanding the full impact on the whole body of inter-related Regulations and Standards becomes problematic. We would encourage NERC to do whatever they can to add timeliness and clarity to this process. Section.5.1 (Physical Facilities) of the proposed standard discusses “not regulated by the NRC or the CNSC”, should include the following clarification “under 10 CFR 73.54”.. Balance of plant (BOP) scope is currently regulated by the NRC under 10 CFR 50.62, 10 CFR 50.63, and 10 CFR 50.65. Without the clarification, the CIP Standards would apply only to systems, structures and components (SSCs) not

Organization	Question 13 Comments (Response page 25)
	regulated under any NRC regulation. 10 CFR 73.54 is the regulation that applies specifically to cyber security. In addition the use of the term "facilities" throughout the CIP standards introduces an element of ambiguity and confusion when applicable entities are attempting to determine impacted systems, structures and components (SSC). We suggest that the SDT refrain from using the term "facilities" and begin introducing "systems, structures and components (SSC)" into the standards.
BPA Trans	Other Comments not already provided in response to earlier questions: First, it is difficult to address this Standard completely without understanding, at least at a high level, how it will interact with the revisions of the remaining CIP-003 through CIP-009 Standards. In particular: 1. Will the standards consider not only impact, but probability? The current standards do not allow any consideration of the probability that a particular vulnerability can and will be exploited. Instead, all threats are treated as being equally probable. As a result, considerable effort could be expended in protecting against threats that are extremely unlikely. 2. Will the entities have the ability to consider the level of risk after mitigation in determining whether to apply a requirement? Currently, the standards give no such flexibility, except for a limited range of Technical Feasibility Exceptions. As a result, strict compliance is required in almost all cases, even where compensating controls have reduced the level of risk to one commensurate or lower than the residual risk after applying the standard. 3. At a high level, what will be required for compliance at each BES Cyber System Impact Level? 4. Will there be any requirements levied on Low Impact BES Cyber Systems? As the impacts are presently defined, it would be hard to justify any such requirements. Low Impact BES Cyber Systems, by definition, can have no impact on the BES. However, the standard does not address that issue.
HQT	Recommend that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." to this version. Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline.
CCG	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot.
Allegheny Energy	• CIP-002, version 4 represents a radical departure from the previous versions. The transition from the approach in version 3 to version 4 is likely to be confusing and result in an abundance of new interpretations. We are concerned about the level of cyber assets that could now be interpreted to be in scope and not add to the reliability of the BES. • We suggest that a new version 4 simply take the existing version 3 and with a modified CIP-002-3 R1.2 that includes some of the specific items in the CIP-002-4 attachment 1 document. This approach would result in an expanded Critical Asset scope with a new implementation plan and would act as a step between V3 and the proposed V4. We also recommend that this stepping block approach address the widely recognized issues with CIP-003-3 through CIP-009-3 such as white-listing device categories,

Organization	Question 13 Comments (Response page 25)
	inconsistencies in TFE applicability within a given requirement and that version 4 include language covering all interpretations from previous versions that remain applicable. • This individual standard cannot be fully reviewed and commented on without reviewing the revisions that are being made to the related CIP-003 thru CIP-009 reliability standards. Further commenting and approval of this standard should be deferred until drafts of all the standards have been completed and made available for review. (For example what will be required of things categorized Low, Medium, High?) • The definition of "Engineering analysis" to get around the hard limits (1,000, 2,000) is too vague and re-assigns the responsibility for determining what is acceptable to the regions. This could create vastly differing interpretations among the various regions. At a minimum, more detail should be provided on what types of “engineering evaluations” for the GO and GOP would be acceptable to the Reliability Coordinator. • Because CIP-002 is so integral to the other reliability standards CIP-003 through CIP-009, this standard should not go into affect until "after the 1st day of the eighth quarter after regulatory approvals have been received for the revision of all CIP-002 through CIP-009". • The previous versions of CIP-002 specifically address only cyber devices that are accessible or can be accessible outside the physical location of the device. This was removed in the current draft. This should be should be put back in. Devices that are not externally accessible can adequately be protected, like any other piece of equipment, solely with physical security.
KCPL	No additional comments
MidAmerican	MidAmerican Energy Company supports modifying all the CIP standards to address the modifications in FERC directed Order 706. In response to FERC and industry concerns regarding identification of assets in CIP-002-1, a summary of revisions MidAmerican supports follows: (1) Change CIP-002-2 R1 to eliminate the risk based methodology and instead list all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards. Consider very limited exceptions. (2) Change CIP-002-2 R2 to “reviewing the list of BES assets” instead of “developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required” as currently written in CIP-002-2. (3) Change CIP-002-2 R3 to use “the list of BES assets” instead of “the list of Critical Assets.” Retain the sub requirements with the qualifying criteria that consider routable protocol or dial-up accessibility. (4) CIP-002-4 cannot be implemented without the revised security controls . (5) Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. Security control categories are dependent upon what the security control is. Development of meaningful categories must be addressed simultaneous with development of the security controls. Moving categorization to the security controls standards gives the industry the opportunity to move forward with CIP-002. (6) Revise CIP-003 through CIP-009 within their existing framework as much as possible. Incorporate categorization discussed

Organization	Question 13 Comments (Response page 25)
	above, where applicable and meaningful. Provide more flexibility in the controls. Replace zero-defect quality prescriptions in the requirements, measures and violation severity levels with results based performance objectives. Explanation and details follow. Criticisms of the results from the existing standards are: not enough Critical Assets and Critical Cyber Assets were identified, and security controls are inflexible. The root causes of these unacceptable results are: (A) CIP-002-2 is not prescriptive enough. (B) CIP-003-2 through CIP-009-2 are too prescriptive, one-size fits all and the associated measures and violation severity levels prescribe zero-defect quality. MidAmerican submits that revisions within the existing framework of the standards will achieve the desired results more effectively and much faster than the significant framework changes proposed. (1) CIP-002-4 as proposed requires all BES all BES transmission lines, substations, generation resources and transmission control rooms covered by NERC standards to be in CIP scope. It addresses the criticism that entities did not include enough assets. MidAmerican supports modifying CIP-002-2 R1 to eliminate the risk based methodology and instead list all owned BES assets (100 kV and above): transmission control centers that are subject to other existing NERC standards, transmission substations and generation resources. A very short list of objective, specific criteria for excluding an asset from CIP should be considered. For example, exclude wind farm generating units when the reliable operation of the grid doesn't yet rely on the wind blowing. For example, exclude small generating units under a certain MW nameplate unless the unit is in the primary black start unit because the other small units have minimal risk of contributing to success of a concerted, well-planned attack against multiple points. This bright line criteria sets the same bar throughout the industry. It eliminates the risk based methodology in CIP-002-2 and the proposed engineering evaluations or other assessment methods (and their associated third party approval) in the proposed CIP-002-4. Both current and proposed methodologies have raised concerns and criticisms and compound complications in the CIP standards. Using existing BES definitions leverages and compliments the rest of the NERC standards. (2) Modify CIP-002-4 R2 to "reviewing the list of BES assets" instead of "developing a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required" as currently written in CIP-002-2. BES bright line criteria also eliminates the need for proposed CIP-002-4 R2 that addresses directly interconnected assets. All assets are held to the same bar across the industry. (3) Change CIP-002-2 R3 to use "the list of BES assets" instead of "the list of Critical Assets." Retain the concepts of and definitions for Cyber Asset and Critical Cyber Asset. Require inventory of Cyber Assets and Critical Cyber Assets for all BES Assets. Security controls are ultimately applied to distinct, discreet Cyber Assets, not to a collection called a "system." Retain the qualifying criteria that consider routable protocol or dial-up accessibility because these are the characteristics that create the vulnerabilities to concerted, well-planned attacks against multiple points. CIP-002-4 R3 as proposed creates a new concept of BES cyber system for use in categorization of security controls.

Organization	Question 13 Comments (Response page 25)
	Categorization level determinations should be addressed in the security control standards. See (6) below. (4) CIP-002-4 cannot be implemented without the revised security controls . The implementation plan has to incorporate transition planning for Cyber Assets currently covered by CIP, if their security control requirements change under the revised standards. (5) Incorporate security categorization level determination in the security control standards, CIP-003 through CIP-009, not in CIP-002-4. MidAmerican submits that the security controls work must be completed to determine what categorizations are possible and needed. MidAmerican has reviewed the existing controls and observes the following. Many security controls are either applied or they are not. Differentiating between high, medium and low may have little value or credibility for many controls. When differentiation is possible and reasonable, the criteria for high, medium or low categorization often has little correlation to the size of the "iron" (substation or generating unit) the cyber asset supports. High, medium or low categorization often has more to do with the connectivity of the asset (TCP/IP vs. dial-up vs. not connected) and/or the span of control of the cyber asset's impact (if it fails, is just one asset impacted or many) in the event of a concerted, well-planned attack against multiple points. For this reason, MidAmerican recommends proceeding with revisions to CIP-002-2 as listed in (1) through (4) above, but moving the categorization aspects of CIP-002-4 into the development of security controls. Categorizations based on analysis of the specific security controls will result in meaningful categories that can be effectively implemented. Where meaningful high, medium or low categories are identified, their criteria should be bright line. For example, authentication for electronic access to a cyber asset is a security control. A Cyber Asset connected by IP and capable of shutting down all the firewalls would be in the high authentication security control category based on its connectivity and span of control. In this case, two-factor authentication might be on the list as one, but not the only, acceptable method to achieve the objective of high electronic authentication security control. Contrast this to a different Cyber Asset connected by dial-up and capable of only impacting one substation. This Cyber Asset would be in a low authentication security control category based on its connectivity and span of control. In this case, use of a password might be on the list as one, but not the only, acceptable method to achieve the objective of low electronic authentication security control. For example, alerting and responding to alerts for unauthorized access attempts to the Cyber Asset access point for the ESP are security controls. An access point Cyber Asset that is dial up and controlling just one 161 kV substation's ESP would be in the low authentication security control category. In this case, reviewing the access point's log every 90 days might be on the list as one, but not the only, acceptable method to achieve the security control objectives of alerting and alert response for unauthorized access attempts to the ESP. In contrast, a routable protocol firewall access point Cyber Asset to transmission control center's ESP would be in the high authentication security control category. In this case, reviewing real-time alerts with immediate response might be on the list as one, but not the only acceptable method to achieve the security control objectives. When the security control objectives and the list of acceptable controls by high, medium or low are determined, it is likely we will find that the level of detail and/or the specific details prescribed by the proposed Attachment 1 may not fit and have to be redone. For this reason, MidAmerican submits that the development of Attachment 1's concepts be concurrent with the security controls work. (6) Revise CIP-003 through CIP-009 within their existing framework as much as possible. MidAmerican supports the Standards Drafting Team's key principle to provide flexibility in applying equivalent security controls on the basis of compensating measures,

Organization	Question 13 Comments (Response page 25)
	cyber system characteristics and operating environment considerations. Analysis of the technical feasibility exceptions submitted in January 2010 should serve to underscore the importance of tailoring security controls between computers (desktops and servers) versus industrial controllers (relays and controllers) versus telecom gear (firewalls and switches). Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with performance based targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented; program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120); and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented; high-controls not implemented; moderate-reviews not completed; lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
CPG	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot. In addition, time and effort should be given to development and consideration of a “cyber first” approach. We appreciate that the proposed version seeks to protect the assets most critical to the bulk electric systems. However, the direction of this proposal may be missing some vulnerabilities and drawing some assets into scope that have little if any impact on reliability. For any approach taken, it is important to remain focused on reliability.
Santee Cooper	Other Comments not already provided in response to earlier questions: No one knows the elements and assets of a company better than the company itself. If we are considering changing this standard, it needs to be simple and absolutely clear. IF it is not clear, then it is left to the interpretation of regional entity and their audit teams. Without intimate knowledge of that company’s system and assets, any room for interpretation would render an unjust burden on that company.
OGE	• Reliability Coordinator or Regional Reliability Assurer should provide a list of groupings of pre-approved engineering evaluations or other assessment methods. As stated, it is possible that the RC/RRA will be inundated with methods and could back-log in approvals, forcing RE’s out of compliance. • Throughout the document, the “engineering evaluation or other assessment method” is referenced. The standard should designate that only the Responsible Entity is authorized to perform the engineering assessment to evaluate the BES Subsystem’s impact. The method may be approved by the RC or RRA, but it should be applied by the Responsible Entity. • OGE proposes that the remaining standards be at least published for informal comments before the formal comment period on CIP-002-4. We need some idea of the controls SDT will be proposing in the following standards (what are now CIP-003 through CIP-009) before informed comments on proposed standard in CIP-002-4 are submitted. • Routable protocol or dial up accessible should be considered as method to limit the universe of BES cyber assets.

Organization	Question 13 Comments (Response page 25)
	• SDT should develop language that allows for the evaluate events based on single contingency • A Readiness audit prior to mandatory date should be performed without the threat of penalties. • SDT should allow for consideration of the "Financial impact" of risk mitigation when the threat is clearly inconsequential. • SDT should develop an awareness roadmap to help change the internal compliance culture as we migrate from Version 1,2,and 3 to Version 4. Many of the original concepts and terms are changing making the transition more difficult. • SDT should state how/why Version 4 increases BES security posture. • Overall we need greater clarity with the requirements to understand exactly how to meet the requirement. The terminology is vague and prone to misinterpretation. • Establish a "No Impact" category for those cyber assets that cannot be compromised by a cyber threat and that do not affect the bulk electric system? • Comments for CIP 002-4 should be requested at the same time as CIP 003-4 through CIP 009-4. • SDT should provide feed-back to these comments before final draft is submitted for comment in late Feb to avoid repeating many of the same comments during the 45 day formal comment period. • Define the "Bright line" and its purpose • Develop a detailed glossary of terms used in the drafting process and in the final requirements. It is very hard to provide the SDT with feedback without understanding the terminology. There is too much subjectively. • We need to be allowed to perform a risk assessment on the BES cyber device to determine if it could impact the electric asset(s) and in cases where the cyber risk below a certain threshold to the BES, then eliminate the device from consideration.
PPL Supply	Agree with EEI Comments. Also, Moving into the future, • We believe that standards development team should focus on the "What" of security control outcomes rather than the "How". • We suggest that the standards drafting team carefully consider issues of flexibility, sustainability, scalability, and repeatability when identifying options for security controls.
NGRID	• National Grid recommends that the Drafting Team adapt the telecommunications exclusion (4.2.2) in CIP-002-1, "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." to this version. • It is also advisable to have a FAQ/Guideline and move the examples into the FAQ/Guideline • National Grid believes that this standard partially represents the whole effort. Because this approach is so radically different it is

Organization	Question 13 Comments (Response page 25)
	critical that the SDT presents a complete package (CIP-002 – 009) for balloting.
MGE	An entity may have a blank list for High and Medium BES Impacts for attachment 1 but several items listed under attachment 2. Is it the intent of the SDT that if an item is listed on attachment 2, that it is a High or Medium BES Impact? Please clarify. We recommend that the SDT add a No BES Impact category along with High, Medium, and Low. If this Standard becomes enforceable, all cyber assets will fall into a Low, Medium, or High category. It is unreasonable to ask the industry to provide comments on this version of this standard without full clarification of High, Medium and Low and what the implications of those ratings are, without posting the proposed CIP-003 through CIP-009 at the same time. CIP-003 through CIP-009 may imply requirements unjustly. Please clarify. Upon reviewing this proposed Standard I kept asking myself "what threat are we guarding against"? Without knowing what the threat is, it is hard to defend or protect a BES cyber asset. One of the first rules in defending anything is to know the capabilities and limitations of your Aggressor.
FE	1. FE supports the expedited schedule for completing a new CIP suite of standards. We recognize the importance of this project and are committed to support completion by Year End 2010. 2. FE believes the industry should submit a complete suite of CIP-002 through CIP-009 standards. Trying to ballot CIP-002 ahead of the other standards presents problems for industry in regards to a complete understanding of expectations and impacts. Balloting CIP-002 ahead of the other standards presents coordination challenges in regards to an effective implementation plan. 3. FE encourages the team to reconsider the purpose of this standard as described above and believes the intent should be on identifying cyber vulnerabilities that could lead to High BES Impacts with appropriate H/M/L cyber asset controls based on the technology in use. A bright line of what will be considered High BES Impact threats should be the focus of Attachment 1. 4. FE does NOT support the work required in Attachment 2. The intended use of the information is not clear.
TECO	We support EEI's comments 1 – 8. In addition, we offer the following as input for consideration. TEC recommends reconsideration/removal of Shared Element as the definition of Element of the BES makes all of the Transmission system except radial transmission lines either a High or Medium. TEC would appreciate additional clarification of the terminology: "could hinder restoration to a normal condition." Routine restoration? Restoration following hurricanes, ice storms, etc? TEC has concerns that the list of assets required for compliance with the currently stated draft does not exist for any utility in the country (every span, protective relay, circuit breaker, etc. associated with a BES Subsystem). Creating such a list and keeping it up to date would require significant effort, documentation, coordination, etc. In addition, TEC strongly supports the following joint comments provided to the utility industry as it relates to the cyber first review of assets. We have incorporated those comments here: • Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of

Organization	Question 13 Comments (Response page 25)
	reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective. • The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. • Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. • CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. • The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… • The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below. Validity of the "Cyber First" Approach to Defining Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – system stability is the salient issue. • N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a coordinated multi-site attack, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on a perpetrator's ability to navigate across and between control system data networks in order to access multiple sites. • "Routable protocol" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented). • Thus, routable protocol networks are the correct object of cyber protection concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.] • At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that do not run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence in practice do not pose a salient threat to BES reliability through cyber means.

Organization	Question 13 Comments (Response page 25)
	• CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for all control cyber assets that communicate in common on a TCP/IP-based data network infrastructure; regardless of how big or small the grid operating site is in terms of electrical rating. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities relevant in practice to BES reliability. • If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is not for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not be imposed where cyber threat is not real. • Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the different Categories of cyber assets as characterized below. Identifying Specific Cyber Objects of Protection • Start by identifying the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement, execute, or support the Essential Functions. • Generally speaking, process and distributed control system elements at work at different types of grid operating site present three major cyber asset categories in terms of cyber risk exposure to the bulk electric system: o Category 1 (High): Control/data/operations/systems administration center cyber assets that employ TCP/IP to communicate; these require the most rigorous cyber security controls and countermeasures because nefarious root capture of control system hosts represents the worst case scenario. o o Category 2 (Medium): "Field" substations, dams, generators, etc., cyber assets that use TCP/IP to communicate; and, cyber assets anywhere that employ dial-up methods regardless of other communications protocols in use. Dial-up aside herein, these cyber assets require earnest cyber security controls and countermeasures, but nefarious root capture of same typically does not directly represent the same grid threat severity as do control system host computers themselves. o o Category 3 (Low): Cyber assets in use at all other operating sites that do not employ routable TCP/IP protocols to communicate. These should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc). • Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset identified above. More granular refinement of cyber security control and countermeasure Requirements will be necessary beyond the gross categorical illustration above, especially concerning Category 2. • Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not

Organization	Question 13 Comments (Response page 25)
	in terms of facility size/rating] • All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I. Advantages of the Recommended Approach • It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The subject is computers, not electricity. • This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's complimentary improvement, not do-over.
Snohomish	The Public Utility District No. 1 of Snohomish County ("District") support many aspects of the CIP 002 version draft. The focus on electric system impacts and the graduated risk levels should allow the electric industry to better focus resources on defending against the greatest risks to electric system reliability. However, we have a number of concerns with the MW thresholds that are used. Consistent with the many issues around the "bright line" voltage based definition used in the Bulk Electric System, the 1000/2000 MW/MVA thresholds do not accurately identify impact risk. "Control Centers and backup Control Centers controlling transmission assets or generation of 1,000 MW or more, not included above." "Each Generation Subsystem with aggregate rated name-plate generation of 1000 MVA or more, not already included in section 1 above, unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support." We prefer a more performance-based approach for both loss of load and generation - such as a utility or region cannot adversely impact neighboring systems. It is very likely that a wind or ice storm could impact 1,000 MW, by faulting key facilities. These types of conditions occur seasonally and should be classified as impacts to local customer service or Level of Service ("LOS"). On the other hand it is possible that facilities less than 1,000 MW may produce wide spread cascading. We suggest that the systems are tested on a system by system basis using TPL, and expanded TPL system assessments. If the facilities do not cause uncontrolled cascading and destroy equipment it should not be considered a reliability impact. However, a compromise may be to classify system categories by MW thresholds to determine the level of assessment that is needed to demonstrate level of BES impact. Such as less than 300 MW requires a powerflow assessment and 300-1,000 MW requires a powerflow and transient stability assessment, and greater than 1,000 MW requires expanded TPL assessments. This expanded assessment may include multiple simultaneous contingency evaluations that would simulate an orchestrated attack on various facilities. It should be noted that load loss should not be the threshold, cascading should be the threshold. The reason is we must benchmark the electric system performance against wind/ice storms and other natural and reoccurring events. If the system does not cascade out and the electric system (equipment is protected/isolated) load can be restored, we believe the system met its performance obligations. If the performance requirements are higher than this the electric industry will treat CIP risks at a much higher level than the seasonal risks that threaten our electric system on a continual basis. As noted above the District believes the engineering evaluations should be applicable to load areas levels as well as generation level

Organization	Question 13 Comments (Response page 25)
	(below). " …unless it has been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage or frequency support." A preferred alternative: "…unless it has been determined not to produce wide spread cascading and is essential to the wide area [adversely impacts neighboring electric utilities] reliability of the BES through an engineering evaluation or other assessment method approved by the Reliability Coordinator or Regional Reliability Assurer, either for voltage, thermal, or frequency support. The District thanks the CIP-002 drafting team for the opportunity to comment.
CECD	In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit -002. After that time, a packaged set of CIP standards should be presented for ballot.
MRO	We believe the intent of the current version of standard CIP-002-3 has a better security focus than the proposed version 4, and that the current version of standard CIP-002-3 should either be maintained, or combined with certain aspects of the version 4 proposal. The current version of standard CIP-002-3 identifies BES sub-systems that are critical to the reliability of the BES, and then proceeds to identify cyber systems critical to the operation of the BES sub-systems. It then goes one step further by differentiating between routable and non-routable connections to these cyber systems. We believe this differentiation is extremely important, since non-routable connections (or even better, eliminating connections wherever practical) are inherently more secure against, and limit potential damage from, remote attacks. This seems to be a straight forward and direct approach to securing the BES from cyber attack, and we do not see any reason to deviate, especially when you consider that version 4 appears to be migrating away from the core scope of protecting against remote cyber attacks. If the concern is too much latitude in the current version of standard CIP-002-3, then the new Identifying Critical Assets and Identifying Critical Cyber Assets guidelines should be rolled in to the current standard as core requirements instead of references, assuring that all entities identify critical assets under a similar, Engineering study based assessment. Completely replacing the existing standard with the entirely new approach of version 4 does not appear to be prudent, as it undoes much of the groundwork laid by the existing standard that directly addresses BES security, especially when the version 3 Identifying Critical Cyber Assets guideline is currently out for formal comment at the same time.
GTC	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards.

Organization	Question 13 Comments (Response page 25)
	2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary? c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could be lowered if certain protective criteria were met (encryption etc.). 5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas should produce a superior set of standards.

Organization	Question 13 Comments (Response page 25)
	6. With respect to section 4.1 of the Standard, the second sentence, beginning "In situations where . . . ," should be deleted as unclear and unnecessary.
Tallahassee	TAL agrees with and supports the comments submitted by the APPA.
BGE	We believe that load management systems should be treated on par with generation resources. If requirements include generation units of a certain size, then load management systems of equal or greater value should also be included. According to Attachment 1, part 1.6, "Each Transmission Subsystem comprising the Cranking Paths" is considered "High BES Impact". Does the drafting team intend for switchable load-serving substations normally tapped from the Cranking Path to be included in the "Transmission Subsystem"? We note that in Attachment 1, part 1.1 (as well as in other parts of Attachment 1) that language is included that allows for engineering studies to be performed in order to demonstrate that a particular asset is not "High Impact". The standard states that the "engineering evaluation or other assessment method" must be approved by the Regional Reliability Assurer or Reliability Coordinator. We agree with the concept of allowing studies to show that an asset is not "High Impact". However, we believe the standard should address the criteria by which the RC or RRA would evaluate and approve a given evaluation. There should be more structure so that the RC or RRA decision to approve or reject a particular study is objective and not subjective. The prior version of CIP-002 considered two dimension of risk for critical cyber assets. The first risk considered impact, whether or not a cyber asset was associated with a critical BES asset. The second risk considered vulnerability by whether or not a cyber asset was accessible by dial-up or routable protocol. The intention to move away from all-or-nothing controls is a favorable evolution, but in this initial proposal the SDT has eliminated any consideration of the dimension of vulnerability from the standard. It is doubtful that the goal of establishing practical and appropriate controls can be done without it. We would suggest that various categorization of vulnerability be designated in CIP-002 (High, Medium, Low or High, Low, No) and the sorting criteria be established in an appendix, similar to Attachment 1 of the current proposal that correspondingly deals with the dimension of impact. As well, understanding the design basis threat against which mitigation measures may be built is fundamental in creating an effective set of control measures. The threat potential basis should be clearly established. In terms of the standard development process, it is critical that stakeholders have the opportunity to evaluate the security controls before accurately commenting on categorization proposals. CIP-002 should not be presented for formal balloting on its own. Sufficient time should be allowed for industry to evaluate revisions to the security control measures and revisit CIP-002. After that time, a packaged set of CIP standards (including proposed revisions to CIP-003 to CIP-009 as they are currently known) should be presented for ballot.
Springfield, MO	City Utilities of Springfield, Missouri is in agreement with comments provided by the APPA Task Force on this question. Additionally, we suggest that the drafting team clarify that each BES Cyber System impact evaluation/assessment is limited to a single BES Cyber System and not multiple BES Cyber Systems.
FPL	We appreciate the hard work from the drafting team and support their efforts to ensure the reliability of the BES. The team has a difficult task in light of pressures from industry as well as Congress. We would like the drafting team to continue considering that the requirements drafted to secure the systems are appropriate to the risk. When considering BES subsystems impact, the level of risk should be commensurate with the amount of work needed to mitigate that risk. That is, in the case of low impact BES subsystems, we should

Organization	Question 13 Comments (Response page 25)
	consider the amount of work relative to the additional security relevant to the security of the BES. The focus should be kept on mitigating risks for remote and physical access with special attention on remote access vulnerabilities when there is connectivity.
TAPS	TAPS supports APPA's proposal submitted in response to this question that "the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment." To do otherwise would prevent stakeholders from voting in an informed manner.
Allegheny power	AP believes that a single package should be put forward that includes both the proposed standard for BES Cyber System Categorization, as well as the associated controls. This is the only way to allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. Moreover, FERC has signaled that it is unlikely to approve a new CIP-002 in the absence of associated controls. AP agrees that there is value in identifying clear and straight forward bright line criteria for high, medium, and low impact BES assets. The bright line criteria should be subject to an approved engineering evaluation in the event that an entity owns or operates an asset that while meeting certain criteria, does not affect the BES to the level indicated by the bright line. AP believes that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility exceptions (TFEs). AP believes that the current written definitions for high and medium impact BES systems do not bring sufficient clarity for determining the appropriate category. AP recommends using only the criteria identified in Appendix 1 to make such determinations. Critical Assets, Cyber Assets and Critical Cyber Assets – These terms should not be replaced. Thousands of hours have been spent developing policies, procedures, job-aids and training programs based on these terms. In addition thousands of hours have been spent training employees, vendors and contractors on cyber security controls based on these definitions. Eliminating these terms will make most of that effort valueless. The program should be focused on strengthening our security position from where we have gotten today. Changing terms will not improve the program, but will ultimately weaken it as there will be confusion and time wasted redoing what has been done over the last 3-4 years. There are typically multiple alternatives for blackstart cranking paths, which can be a benefit to system restoration. The standard needs to specify the "primary" cranking path. Also, there may be numerous blackstart generating units listed in a blackstart restoration plan which are not specifically identified as being utilized by the restoration plan. The standard needs to be more specific concerning how blackstart units are identified in the restoration plan. For example, blackstart units not identified in the restoration plan as part of the "primary" cranking path should not be considered as high or medium impact BES Subsystems. AP would like to see controls revised to continue to have appropriate qualification based on use of routable protocols or networks that communicate outside the Electronic Security Perimeter.
FMPA	We applaud the effort to develop a uniform risk based assessment methodology for the industry. We believe that the direction is good, it is the details that we disagree with. We believe that a lot can be done to simplify and make less ambiguous, such as eliminating the concepts of functions and Subsystems and instead just focusing on worst case contingency / scenarios that can be caused by malicious

Organization	Question 13 Comments (Response page 25)
	use of a Cyber System and comparing those scenarios to the good start made in Appendix 1. There should be the ability to avoid doing any analyses or any comparison against criteria if an Entity already believes that one of the Cyber Systems they own has a High BES Impact specific to that Cyber System. The analyses and comparison against criteria should only apply to its Cyber Systems that the Entity believes are not High BES Impact. Independent 3rd Party Review FMPA is encouraged by the tiered approach to cyber-security proposed by the SDT, but is concerned that any bright-line metrics must be based on operationally sound regional parameters for BES planning and operations. We agree that use of entity-specific parameters concerning the classification of BES systems should be avoided, because this triggers the same difficult study issues that proved problematic during the identification of Critical Assets under CIP-002-1. However, while the need for entity-specific studies is reduced by using "bright line" regional metrics such as Contingency Reserves and IROLs that define normal and emergency operations, we cannot completely eliminate the need for entity-specific and sub-area studies, which may raise an issue concerning third party independent review of these entity-specific or sub-area studies. Many regional "fill-in-the-blank" standards raise similar issues. For example, the UFLS Standard Drafting Team, in its efforts to determine who should perform region-specific UFLS studies (e.g., to determine how much load to shed at what frequency and with what time delay), is considering a proposal to create a new Registered Entity called the “Regional Planning Coordinator Group.” Such a Regional Planning Coordinator Group could be useful to other standards as well, and could be the "right" entity to perform independent third party reviews. For these reasons, FMPA recommends that the CSO706 SDT propose to create a new Registered Entity called the “Regional Planning Coordinator Group.” Similar in concept to a Reserve Sharing Group, all of the Planning Coordinators in a region would be required to become members of the Regional Planning Coordinator Group and would be required to perform and/or approve regional studies. The Regional Planning Coordinator Group would also be charged with the review and approval of studies by individual Registered Entities that propose to depart from the regional parameters and bright-line criteria approved under Attachment 1. The approach outlined above addresses regulatory directives that NERC standards not assign responsibility to comply with standards to the same entity that is responsible for assuring compliance with standards, while ensuring that the entity or entities responsible for performing regional studies have a wide-area perspective and the capability to fully assess the impacts of planning and operating studies. The Process for Industry Approval of CIP-002-4 Must be Synchronized with CIP-003-4 through CIP-009-4. We believe the industry the industry will find it difficult to reach consensus in support of CIP-002-4 and address all of the technical issues raised by this standard prior to its review of the associated security controls being developed standards CIP-003-4 through CIP-009-4. CIP-002 through CIP-009 cannot be taken one at a time. FMPA recommends that the SDT should incorporate the industry comments received in the informal comment period on this draft of CIP-002-4 and then begin to draft CIP-003-4 through CIP-009-4, using a revised draft of CIP-002-4 draft as a new baseline. The SDT should then post the entire suite of draft standards, including the whole CIP-002 through CIP-009 series of standards for a second round of informal industry comment. Under this revised development plan, the industry will have the opportunity to understand the whole suite of standards before they vote to give final approval to CIP-002-4. FMPA would support an industry-wide straw vote to garner conceptual approval of the next version of CIP-002-4 standard. Once so

Organization	Question 13 Comments (Response page 25)
	approved, the draft CIP-002-4 could be provided to the FERC and other regulatory bodies either on an informational basis or for conceptual approval. Such conceptual approval by industry and regulators would give the industry, the SDT, regulators and Congress greater confidence that NERC is making strides to complete this project expeditiously, while ensuring that the target end-state will be acceptable to stakeholders and government authorities.
Duke	We believe that the proposed CIP-002-4 is too prescriptive, and that a better approach would be to use the "Cyber First" approach. Also, we believe that it is essential that the other CIP standards should be revised and balloted in concert with CIP-002-4. The "Cyber First" approach should begin with identification of Cyber Systems that can impact BES reliability. The Cyber Systems should then be categorized based upon both their potential adverse impact and risk, and protection requirements established accordingly. For example Cyber Systems that are part of a routable protocol communication network are considered to have highest risk because of their potential "reach". But serial and dial-up communications could also be compromised and attacked in concert to impact multiple BES System facilities at once, so they must also receive appropriate consideration and protections. This approach to cyber security continues and builds upon work already done by the industry.
AESI	1. We disagree with the approach the SDT is taking. We believe the advantages that will be attained from the greater granularity provided in the proposed revision will be more than outweighed by the complexity introduced by having multiple levels of requirements. Conducting a rewrite of this magnitude will also render useless much of the clarification and understanding that has been very painfully gained through implementation of the current revisions and all the formal and informal discussion and interpretation that have been conducted. We will be starting back at square one with a new set of words which will inevitably bring a new set of ambiguities and unforeseen scenarios. We believe that FERC Order 706 could be better addressed through an incremental revision to the standards. 2. CIP-002 cannot be considered independently of CIP-003-009. The proposed revision would constitute a tradeoff between simplicity and granularity. The challenges of dealing with increased categories of systems are clear (and in light of our struggles with the current standards are rather daunting). We definitely see a potential benefit in granularity, but the degree to which that will be realized is dependent on the details of how the remaining standards are rewritten. We are being asked to vote on a change when we have been given a good picture of the substantial associated costs (having to deal with multiple categories of equipment, records, and requirements), but only a vague sketch of the benefits (hopefully reduced scope of requirements for many assets). Further discussion on CIP-002 should be held in abeyance until the rewrite of the other CIP standards is completed. 3. The exclusion for communications between ESPs is not present in this version and should be reintroduced. To expand covered systems in this dramatic fashion is not a worthwhile allocation of scarce resources. The premise of an ESP is that activity from outside its borders should not be trusted, so application of the standards to those assets is not needed. It also raises several issues regarding the scope, including: a. To what extent are services and equipment provided by third parties covered? b. If services and equipment provided by third parties are not covered would the definition of a third party include a subsidiary or affiliate, i.e. could an entity escape the standards by placing its communication assets under the operation of a subsidiary?

Organization	Question 13 Comments (Response page 25)
	c. To what level of communication equipment do the standards apply? Do you really intend to include a company's backbone fiber telecommunications networks as a BES cyber system? If a communication path transits through a switch within a VLAN or VPN is that switch a BES cyber system? What if there is an alternate route available? 4. The proposed standard inappropriately treats cyber assets the same regardless of their risk profile in direct contradiction of the SDT's stated goal of avoiding one size fits all requirements. The current version of CIP-002 implicitly includes a consideration for the risk associated with a cyber asset in the determination of whether it is a critical cyber asset. This was done by limiting the definition of cyber assets to devices that used dial-up or routable protocol communications. Version 4 eliminates this distinction with the impact of vastly expanding the scope of covered assets. It also results in treating devices with extremely different risk profiles the same. Take the examples of an RTU communicating serially over an encrypted, dedicated, company-owned communication facility, and another RTU serving an identical substation but communicating via an IP connection on the public Internet. In the old standard the first device would be excluded from all requirements because of its low risk profile and the second would be subject to the full set of requirements. But in the new version both would be subject to the same level of scrutiny which would be totally independent of the risk of intrusion. Ironically this is the opposite of the stated goal. We believe that the risk profile of the cyber asset must be reintroduced into the version 4 standards in order to achieve your goal of moving away from one size fits all requirements. Perhaps an initial determination of the impact of a cyber device could be based on the BES Subsystem it is associated with, but that impact could be lowered if certain protective criteria were met (encryption etc.). 5. A specific set of CIP standards for control centers, for transmission assets and for power plants should be considered in lieu of a multilayered single standard. In the majority of utilities these assets are managed by individuals in different departments, often in different divisions, so specific standards for each asset class developed and interpreted by subject matter experts in these areas should produce a superior set of standards. 6. With respect to section 4.1 of the Standard, the second sentence, beginning "In situations where . . . ," should be deleted as unclear and unnecessary.
IESO	In concurrence with the IRC we submit the same response as follows: It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. We are concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their

Organization	Question 13 Comments (Response page 25)
	companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. As discussed in detail with regard to draft Requirement 1.2, we do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. In addition to the shortcomings detailed above, it should also be noted that evaluation of Asset Owners' Cyber Systems falls outside of the RC's expertise. The Commission expressed its concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the registered entity perform the review. How can an RC review the BA it is also registered as? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this problem. It is not clear why R2 is needed.
Manitoba 2	Are the applicable entities the same for all the standards? Are all requirements applicable to all Applicable Entities?
OMPA	The CIP-002-4 approval process needs to be coordinated and in step with the controls portion of these standards; CIP-003-4 through CIP-009-4. It is difficult to accept the proposed methodology and concepts without the ability to see the entire set of requirements for a better understanding of what each impact level would require.
ATC	ATC appreciates all of the work and effort that the SDT has done to develop this standard, but believes that it represents only one piece of the whole effort. Because this approach is so radically different we would not be able to vote for this standard without CIP-003 through 009 being ready at the same time. In other words we believe that the SDT needs to present a complete package (CIP-002 – 009) for balloting. Early Drafts of CIP-003 through 009 would not satisfy our position to only ballot on a complete package. As questions 9, 10 and 11 demonstrate this proposed standards is written with a focus on Transmission and Generation companies with no focus on other entities that may need to comply with this standard. ATC is not against this narrowing of the standard and believes that if the SDT can not write the requirements (Attachment 1) to be more inclusive then they need to drop entities from the Applicability of this standard. One thing that the SDT has to insure is that this standard is only applicable to facilities that are covered under FPA 215 which applies to

Organization	Question 13 Comments (Response page 25)
	the Bulk Electric System. (100 kV and above) We believe that NERC does not authority to write mandatory and enforceable standards beyond that which is authorized under FPA 215. ATC has made a number of edits around this position and we hope that the SDT includes them in the next posting. ATC is offering up two options for the SDT to consider. Building off the existing approved standard (CIP-002-3) 1. Responsible entities shall identify those BES Subsystem that qualify under Attachment 1 as High (i.e. Critical) 1.1. Responsible Entities may remove facilities that qualify as High (Transmission Subsystem or Generations Subsystem) per Attachment 1 if they perform an engineering evaluation / assessment that satisfy Requirement 2. R2. Responsible Entities that develop an engineering evaluation / assessment for 1.1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading, as defined by the responsible entity, beyond the Responsible Entities territory being studied. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) (Please see our examples of a Transmission Subsystem identified in Question 1e.) R3. Responsible Entities shall develop a list of all its Transmission Subsystem, Generation Subsystem and Control Centers, as appropriate, in order to identify its Categorization following R1 and R2. R4. Responsible Entities shall identify blackstart generators and cranking paths per Attachment 1. This approach follows the existing approach by only including those facilities which fall into the “high” / “critical” category. It improves the standard by identifying more clearly those facilities that have to be included as “high” but allows for the necessary flexibility for an entity to take to demonstrate that the assumed BES impact is incorrect. (Please see or modifications to Attachment 1) (NOTE: This would apply to either option.) Second Options is covered in Questions X, X and X but is repeated here for greater clarity. 1. Each Responsible Entity shall categorize the Generations Subsystems, Transmission Subsystems and Control Centers under its

Organization	Question 13 Comments (Response page 25)
	ownership by applying the criteria in CIP-002-Attachment 1…" 1.1. Each Responsible Entity shall update its categorized list(s) (Specified in R1) of Generation Subsystem, Transmission Subsystem and Control Center, as applicable, as a result of the commission or decommissioning of any new or existing Generation Subsystem, Transmission Subsystem within 60 calendar days following the completion of the change. R2. Responsible Entities that develop an engineering evaluation / assessment identified in Attachment 1 must demonstrate that the following items are satisfied and documented: 2.1. Identify the Functions from Attachment 2 with the BES Cyber System being evaluated / assessed. 2.3 A cyber attack on a BES Cyber System associated with an identified Transmission Subsystem, Generation Subsystem or Control Center does not result in BES instability, separation or cascading beyond the Responsible Entities territory being studied as defined by the responsible entity. (Territory allows Responsible Entities that operate non-continues service areas to perform separate engineering evaluation / assessment for each territory) 2.2. Engineering evaluations / assessments allows for the consideration of an entities current security practices and infrastructure configuration (Entities may go beyond the study of impact to document their protections which mitigate the possibility of a cyber attack. (i.e. Private network, encryption software, multiple authentication levels, disconnection from the internet … etc.) 2.3 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Planning Coordinator to support the categorization of BES Subsystems where required by Attachment 1." 3. Each Responsible Entity shall categorize and document BES Cyber System as Follows: 3.1. Each Responsible Entity shall list each BES Cyber System associated with a Transmission Subsystem, Generation Subsystem or Control Center categorized in Requirement 1 for its facilities that qualify as either High BES Impact or Medium BES Impact. 3.2 Each Responsible Entity shall assign the same BES impact categorization (High or Medium) to each BES Cyber System associated with its Transmission Subsystem, Generation Subsystem or Control Center. Attachment 1: Entities may perform an engineering evaluation / assessments as per requirement 2 (ATC Suggested Requirement 2) in order to determined if the Transmission Subsystem, Generation Subsystem or Control Center can be removed from the predefine BES categorization (High or Medium). The engineering evaluation / assessment shall consider those facilities (breakers, tap changes, real-time data) that make up the Transmission Subsystem, Generation Subsystem or Control Centers that could be compromised if it's associated BES Cyber System is successfully attached. In addition, entity are allowed to consider its network infrastructure and security practices as part of its engineering evaluation / assessment. This will allow entities to understand both the impact of the possible compromised against is current security practices and

Organization	Question 13 Comments (Response page 25)
	infrastructure investments. Restoration is treated separately please see the restoration portion of Attachment. High BES Impact 1.9 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 1.10 Each Generation Subsystem whose aggregate output exceeds the largest value of the Contingency Reserve or total Reserve Sharing Obligations 1.11 Each Generation Subsystem that has been pre-designated as Reliability “must run” unit. 1.12 Each Transmission Subsystem which contains Elements that are operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 300 kV or higher in the Eastern and Western Interconnection, or operated at 200 kV or higher in other Interconnection. 1.13 Each Transmission Subsystem that contains Elements which comprise of a defined IROL. 1.14 Each BES Subsystem that performs automatic load shedding of 300 MW or more. 1.15 Each Control Center and backup Control Center performing Reliability Coordination functions. 1.16 Each Control Center and backup Control Center performing BA or TOP functions on Transmission Subsystems or Generations Subsystems that qualify under 1.1 – 1.6. (Note: ATC removed the 2,000 MW level from the SDT number 1.16 because it does not provide any addition clarity. Does the SDT mean to say that if a BA or TOP have a more then 2,000 MW of generation or load within its service territory? As a Transmission only company ATC would not know how to apply the 2,000 MW level. (Does this apply to the MW’s of load or generation) ATC believes strongly that the SDT proposed number 1.13 (Protection System, SPS and RAS) needs to be deleted. We make this recommendation because 1) Protection Systems are covered by our suggested definition for Transmission Subsystem or Generation Subsystem 2) SPS are extensively reviewed and approved so that they do not cause a major impact on the BES. (SPS are reviewed by not only the entity that is installing the SPS by also the Regional Entity in which the SPS will reside. As part of the approval process an entity has to demonstrate that the SPS if either activated prematurely or fails to activate does not cause a major impact on the BES. SPS also have to be reviewed on a consistent interval to insure of their impact and necessity.) Medium BES impact 2.3 Each Generation Subsystem with aggregate rated name-plate generation of 2,000 MVA or more. 2.4 Each Transmission Subsystem which contains Elements that are operated at 200 kV or higher in the Eastern and Western

<table>
<tr><th>Organization</th><th>Question 13 Comments (Response page 25)</th></tr>
<tr><td></td><td>Interconnection, or operated at 100 kV or higher in other Interconnection, with 3 or more Transmission Lines operated at 200 kV or higher in the Eastern and Western Interconnection, or operated at 100 kV or higher in other Interconnection.

Restoration Criteria:

3) Entities that have a single Blackstart unit identified for EOP-005 compliance will have to classify that unit as high.
4) Entities that have a single cranking path identified for EOP-005 compliance will classify all associated substation(s) as high. (A single cranking path is a path that does not have any identified alternative substations in EOP-005 compliance plan.)
5) Entities that have multiple Blackstart units identified for EOP-005 compliance will not have to identify any blackstart unit(s) for this standard.
6) Entities that have multiple cranking paths identified for EOP-005 compliance will not have to identify any of those substations for this standard. (A substation may qualify for High or Low based on other consideration identified in Attachment 1.)</td></tr>
<tr><td>LES</td><td>We support the MRO NSRS comments along with our additional comment found in Question 1.a: (If the industry is determined to change the approach of the NERC CIP Standards, LES proposes there needs to be more emphasis in determining the classification of assets by the connectivity to the outside world. This could be a first step in identifying the assets that need to be reviewed for their impacts. There needs to be consideration placed on the type of communication system being used, private or public, and the type of protocol, routable or non-routable. If utilities try to isolate their systems, install non-routable connections, or remove remote access capabilities to avoid the standards, isn't this a benefit to the security of the BES (i.e. less assets networked together on a common system)? There may be a loss of efficiency from remote management, but aren't we trying to be more secure? It is difficult to take a stand-alone substation system with a dedicated private serial link running DNP and say you need to install systems to remotely manage systems for patches, signature updates, logging, and monitoring. These additional systems will most likely require a routable protocol and will open up a system to remote attack that was originally isolated in the name of increased security! There appears to be many more documented attacks on routable network connected devices, than devices on non-routable dedicated communication links.

It would be prudent for the industry to follow existing industry guidelines for securing Industrial Control Systems such as ISA, ANSI, EPRI, and NIST. The approach to identify the assets needing protection should be based on their risk of remote cyber attack and their impact to the BES. An approach, which is simplified below, is to determine the type of security function to apply based on network connectivity and could be used in conjunction with the level of impact:

(the table could not be submitted through the NERC comment form and was emailed to Joe Bucciero and Lauren Koller instead. Please contact Eric Ruskamp at eruskamp@les.com if you would like an additional copy of the table)
<table>
<tr><th></th><th colspan="7">Security Function</th></tr>
<tr><th>Network Connections</th><th>Physical Perimeter</th><th>Data Encryption</th><th>Antivirus</th><th>OS Patches</th><th>Intrusion Detection</th><th>Account Passwords</th><th>Firewall</th></tr>
<tr><td>Air Gap</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable –</td><td>✓</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Organization</th><th>Question 13 Comments (Response page 25)</th></tr>
<tr><td></td><td>
<table>
<tr><td>Private</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-Routable -Public</td><td>✓</td><td>✓</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Routable - Private</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Routable - Public</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>

Without knowing the extent of CIP-003-CIP-009 Version 4, it is difficult to determine if the standards will be preventing the industry from implementing new engineered solutions. New technologies are being developed that “physically” isolate systems (i.e. unidirectional communications), but the current “flavor” of the standards seem to remove any incentive to implement a more secure solution. If people are of the mindset an “air gap” solution is not secure, the industry is headed in the wrong direction. It is disappointing the industry is being coerced into standards that don’t follow a sound engineering basis for evaluating cost, reliability, and data availability. It seems like the whole push from Congress to get something done is based on the “Aurora Vulnerability” which was misrepresented as a cyber attack, when it really wasn’t (see the NERC MRC presentation for Feb. 15th, 2010).)
</td></tr>
<tr><td>PSE</td><td>Please comment how a regional BES definition impacts the application of this standard. Meaning if an entity deems it has no material impact to the BES and that is "approved" then does that entity need to apply CIP-002.

Specificity is needed in this standard as it is markedly different from general traditional engineering thought and entities need to ensure they are meeting NERC's intent, expectation, and are consistency applying this standard. In addition it minimizes interpretation.

Consider the implementation plan to allow for a grace period as this requirement becomes mandatory or a mechanism that an entity can understand whether they've met the mark by the auditor before being penalized.</td></tr>
<tr><td>IMPA</td><td>IMPA would like the Cyber SDT to consider posting CIP-002-4 for second commenting at the same time they post CIP-003 through CIP-009 for first commenting. This will allow the industry to make comments on CIP-002-4 and know what CIP-003 through CIP-009 might have in them. For balloting purposes, IMPA would like to see all the CIP standards posted for balloting together at the same time (CIP-002-4 thru CIP-009-4).

IMPA recommends a phase in period for implementing CIP-002-4 should be considered. (The first day of the eighth calendar quarter after applicable regulatory approval is the current effective date.) This Standard has the potential to be very costly in terms of manpower and expenses (especially since we don’t know what impact the revised 003-009 Standards will have). A suggestion would be a Responsible Entity has to have 50% of their assets evaluated after 8 quarters, 75% after 10 quarters, and 100% after 12 quarters.</td></tr>
<tr><td>ERCOT</td><td>• ERCOT ISO supports Midwest ISO Comments.
• It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category.
• Title – The title should change to state “BES Cyber System Identification and Categorization” since the Purpose explicitly says “to</td></tr>
</table>

Organization	Question 13 Comments (Response page 25)
	identify" BES Cyber Systems. Also, the verbiage of the 3 Requirements indicates that identification is "assumed" when categorizing. • Section 5.1 Physical Facilities – The use of "BES facilities" is different and inconsistent with "BES Facilities" used in the definition for BES Subsystem. Recommend "BES Facilities" be added to the Definition of Terms and used consistently. The language appears to be an incomplete thought. The language only addressed nuclear facilities. • Effective Date – The effective date should be consistent with the regulatory approval of CIP-003-4 through CIP-009-4. The requirements and terminology across the standards should be consistent and aligned. If this cannot be accomplished, a cross reference of prior terms to new terms should be addressed. (i.e.: critical asset to the new term, critical cyber asset to the new term, non-critical cyber asset to the new term, etc.) • It appears that the new standard relieves Responsible Entities from a periodic review and reaffirmation of their lists when there are no changes to the assets. • An implementation schedule should be addressed for the timeline to implement controls where assets have been reclassified due to the adoption of this new approach. If the current Implementation Plan for New Identified Critical Cyber Assets and Newly Registered Entities is intended for use to determine these timelines, it should be so stated. • Figures 5, 6, & 7 in the concept paper mention a specific vendor's product (PI). While that document is not under review it should be noted that this document should be corrected with a generalized term such as data historian. Midwest ISO Comments: • In general, we do not support the concept of moving from identifying Critical Assets and associated Critical Cyber Assets to categorizing all BES Subsystems and all BES Cyber Systems into one of three buckets that will require some level of protection per standards. We believe that it is far too complicated and exceeds what is needed for reliability and was mandated in Order 706. • It is also very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. Therefore, if this proposed Standard moves forward its balloting should be deferred until the initial balloting of Version 4 of CIP-003 through CIP-009. This deferral should not cause a problem because Version 4 of CIP-002 cannot become effective until Version 4 of CIP-003 through CIP-009 becomes effective as well. • We are also concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the

Organization	Question 13 Comments (Response page 25)
	NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. • The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. • We do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. We believe there are many problems with expecting the RC to perform an external review. For one, evaluation of Cyber Systems falls outside of the RC's expertise. Further, the Commission expressed their concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the Registered Entity perform the review. How can an RC review the BA if it is also registered as the BA? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this situation. • We are concerned about the addition of the function entity Reliability Assurer. While it was added to the most recent Functional Model, we believe it is premature to begin using this entity. While many believe that NERC and the Regional Entities are ultimately the Reliability Assurer, the function model is not clear this is the case. Furthermore, the Functional Model Working Group purposely drafting the Functional Model in a way so that it does not have to be the Regional Entities and/or NERC. Does the drafting team have a vision of whom the Reliability Assurer is? It has not been shared and we believe the drafting team needs to make clear whom they believe serves this role before it is added as new functional entity. Has this addition been coordinated with NERC certification and registry staff whom will have to register and certify this entity?
IRC	It is very difficult to assess the quality of this standard without any idea of what level of security controls are required for each impact category. We are concerned that the drafting team may be inadvertently causing the CIP standards to become applicable to market systems by requiring all BES subsystems and BES Cyber Systems to be categorized and thus impacting market tariffs that have already been approved by the Commission. Market systems allow market participants to interface with ISOs and RTOs. Market participants input data such as bids and offers that are then evaluated by ISO and RTOs to clear the market. These market systems interface with the reliability functions and systems such as state estimation and real-time contingency analysis. When cyber assets were classified as critical and

Organization	Question 13 Comments (Response page 25)
	non-critical, there was no problem because these market systems did not have a significant impact. Now that the drafting team is moving to categorize all BES cyber systems, these market systems will likely be categorized and thus require compliance to the security controls in the NERC standards. (Please note all ISOs/RTOs already have stringency cyber security policies so the issue is not securing the systems but rather demonstrating compliance to the NERC standards which may not be possible for these market systems.) As an example, assuming one security control may be to require personnel risk assessments (PRA) for those with cyber or physical access, this presents a significant problem. There are literally hundreds of users spread across dozens of companies that have access to submit their companies' market information. Would the drafting team propose that the ISO/RTOs now must perform PRAs on all these users? This is both impractical and not necessary as the market user could not realistically impact the BES with these systems and the individual companies have financial incentives to ensure that their personnel are trustworthy. Furthermore, it might not even be legal to require PRAs on all of these users. The drafting team needs to ensure that market systems are not inadvertently drawn into this standard. The discussion above also highlights a fundamental issue with the existing CIP standards regarding cyber access. Many assume anyone who has a user account is considered to have cyber access. However, we believe only those with administrative access should be considered to have cyber access. A user that inputs data can't have a significant impact on the operation of the BES. RCs, BAs, and TOPs already have effective methods that have been used for scores of years to handle bad data. Introduction of bad data by a user is not a significant risk. Executing malicious code by having administrative access is the real risk. As discussed in detail with regard to draft Requirement 1.2, we do not support the reliance on the Reliability Coordinator to conduct any kind of external review, including reviewing the engineering assessments identified in this standard. In addition to the shortcomings detailed above, it should also be noted that evaluation of Asset Owners' Cyber Systems falls outside of the RC's expertise. The Commission expressed its concern is with the fielded assets in order 706-A and not the cyber assets. Paragraph 50 states: "The Commission agrees with ISO/RTO Council that pre-audit external reviews would only review a responsible entity's identification of critical assets and not its identification of critical cyber assets." Secondly, 12 of 17 Reliability Coordinators in the NERC compliance registry are also registered as another function such as a BA. The Commission used the term "external review" in order 706. Thus, one can only assume that the Commission desired to have personnel external to the registered entity perform the review. How can an RC review the BA it is also registered as? Further, who performs the RC external review? Note this is not an exception but rather the rule because the supermajority of RCs fit into this problem. It is not clear why R2 is needed.
PEPCO	1. We support NERC's efforts to develop a complete revised set of CIP standards in 2010, with a plan to file the new set of Standards with FERC in early 2011. We recognized the importance of this activity and are committed to this effort. We believe that the new CIP standards development project is one of the most important activities facing both NERC and the industry in 2010. 2. We believe that CIP-002 -4 should be developed. Balloted, and submitted as a single package with CIP-003-4 through CIP-009-4 NERC. This will allow the industry and FERC to perform an overall impact analysis of the proposed standards, and determine how the standards will affect BES reliability. 3. We believe that the industry should move to a less administrative burdensome process and more of a performance based effort by using the proposed modified cyber approach as previously discussed. The proposed approach would not require classification or identification of big iron, would limit the focus to defined in-scope cyber control systems, and would apply the appropriate security measures/requirements based on specific criteria (e.g. operating platform, connectivity of the asset, span of control of the cyber

Organization	Question 13 Comments (Response page 25)
	asset's impact). 4. We believe that the standards should be written in a way to be able to retire/or significantly reduce the need for Technical Feasibility exceptions (TFEs).
NEI	A) Need to specify screening criteria. B) CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required. Balloting CIP-002 ahead of the other standards presents coordination challenges in regards to an effective implementation plan. C) The process for notification and request for comment needs improvement. Personnel who are site Cyber Security personnel were not aware until after NEI notification. The materials were also not easy to find on the NERC website. D) The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system. E) Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. F) The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"… G) Alternative Top-down argument for defining the correct CIP Standards' Scope of Applicability • "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue. • N-1 engineering also dictates that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability. • Multi-site cyber security compromise is dependent on the perpetrator's ability to *navigate* across and between control system data networks to *access* multiple sites. H) Draft Standard CIP-002-4 dictates that the process of defining scope of CIP Standards applicability is to begin from the frame of reference of electric grid engineering, facilities ratings, and other qualifiers listed in Attachment I. The issue at hand is the cyber security of process and distributed control systems, and therefore should be approached fundamentally from a networked-computing systems security engineering perspective. I) The CIP applicability-scoping process being specified in CIP-002-4 should begin with Requirement 3 and Attachment II, first identifying logical "Functions Essential to BES Reliability." The next step in the process is identification and categorization of

Organization	Question 13 Comments (Response page 25)

	networked-computing cyber assets that implement or enable the Essential Functions as elements/components of a process and/or distributed control system.
	
	J) Three sets of increasingly more stringent cyber security controls and countermeasures (Requirements) should be defined based upon the severity of potential adverse impact to the BES in the event that the cyber assets themselves are lost or compromised. Furthermore, CIP-003-4 through CIP-009-4 control and countermeasure Requirements applicable for each Category must be presented to the industry and balloted concurrently with CIP-002-4, as a set, just as the CIP-00X-1/2/3 Standards development process was executed. Scope of applicability (CIP-002-4) can only be properly considered in light of the specific controls and countermeasures to be required.
	
	K) The single most salient determinate factor in quantifying cyber security risk to reliability of the BES is whether or not a cyber asset is attached in production operation as part of a TCP/IP (routable protocol) control system network. This is the "bright line"…
	
	L) The rationale for a "Cyber First" CIP-002-4 methodology, further digression into related and supporting recommendations, and a brief list of advantages follows below.
	
	<u>Validity of the "Cyber First" Approach to Defining CIP Standards' Scope of Applicability</u>
	
	• "N-1 engineering" has long proven in practice that no single grid operating site is critical to reliability of the BES; electric grid assets functioning in unison as a system is the correct object of infrastructure protection – *system* stability is the salient issue.
	
	• N-1 engineering also has the effect that in order for subversion of the bulk electric system to be successful, it requires a *coordinated multi-site attack*, be it through physical or cyber (or hybrid) means, to effectively adversely impact reliability.
	
	• Multi-site cyber security compromise is dependent on a perpetrator's ability to *navigate* across and between control system data networks in order to *access* multiple sites.
	
	• "Routable *protocol*" data networks (e.g., "TCP/IP") permit network navigation and multi-site attack access (unless proper defensive countermeasures are implemented).
	
	• Thus, routable protocol networks are the *correct object of cyber protection* concerning reliability of the BES. [Likewise so is dial-up communications, but with a more limited set of potential compromises/effects, using different technical and procedural methods.]
	
	• At the same time, it is imprudent to require rigorous cyber defense measures within and between grid assets that *do not* run routable protocols (i.e., they use "legacy serial" communications lines), because they are not navigable, and hence *in practice do not pose a salient threat* to BES reliability *through cyber means*.
	
	• Process and distributed control system elements at work in different types of grid operating sites present three major cyber asset categories in terms of *risk exposure*:
	
	  o Category 1 (High): control/data/operations centers employing TCP/IP;
	
	  o Category 2 (Medium): field operating assets employing TCP/IP (substations, dams, generators, etc.); and, dial-up regardless of other communications protocols also in use;

Organization	Question 13 Comments (Response page 25)
	o Category 3 (Low): all other sites served by cyber control system elements that do not employ routable TCP/IP protocol communications. • CIP-002-1 correctly focuses on routable protocol networking as the primary scope qualifier, but falls short in appreciation of the need for cyber protection for *all control cyber assets that communicate in common* on a TCP/IP-based data network infrastructure; *regardless of how big or small the grid operating site is in terms of electrical rating*. A control host system can be as readily cyber attacked from a TCP/IP-enabled 69kV substation as it can from one rated EHV. At the same time EHV substations connected to control systems only by legacy serial lines, from a purely cyber security perspective, do not pose vulnerabilities relevant in practice to BES reliability. • If certain non-TCP/IP-based grid assets are felt "intuitively" to be critical, e.g., large generation sites, EHV substations, and thereby should be subject to increased protections, this must be done with full recognition that it is *not* for reasons of cyber vulnerability. Increased physical security measures may be appropriate, but rigorous cyber security countermeasures should not be imposed where cyber threat is not real. • Accordingly, the standard drafting team should develop defensive cyber security control and countermeasure requirements in CIP-003-4 through CIP-009-4 that reflect the differences between the above Categories, as follows: <u>Identifying Specific Cyber Objects of Protection</u> • Identify the specific control system cyber assets used to implement/execute the logical "Functions Essential to BES Reliability" listed in Attachment II. These cyber assets include such things as applications, data bases, systems utilities, etc.; computers (e.g., host, server, IED, etc.); and data networking equipment (e.g., routers, firewalls, IDS, etc.) that are used to implement and execute the Essential Functions. • Categorize the specific cyber assets (above) in use into the following subsets: o Category 1 cyber assets using TCP/IP to communicate o Category 2 cyber assets using TCP/IP to communicate; and any others which employ dial-up communications, regardless of what other type of protocol the cyber asset may use to communicate elsewhere. o Remaining cyber assets represent Category 3, and should be subject only to baseline "housekeeping" systems management processes and procedures to assure proper cyber operation (configuration management/change control, "computer maintenance," etc.). • Develop three hierarchical sets (high-medium-low) of cyber security controls and countermeasures appropriate for each Category of cyber asset, as identified above. • Develop VRF/VSL per formula in terms of compliance/deviation from required cyber security countermeasures and controls. [Not in terms of facility size/rating] • All sites require some measure of physical security, and it may be wise to differentiate a hierarchy of physical security countermeasures depending on grid facility size, type, and/or rating, perhaps using Attachment I.

Organization	Question 13 Comments (Response page 25)
	Advantages of the Recommended Approach • It correctly focuses on networked-computing engineering as the primary frame of reference, not grid electrical engineering. The subject is computers, not electricity. • This paradigm continues and leverages the work already done to date by the industry in becoming CIP Version 1 compliant; it's complimentary improvement, not do-over. • It results in application of cyber defenses appropriate to true risk, and does not require expense and effort securing assets that do not pose a genuine vulnerability/threat. • It provides Responsible Entities the autonomy to manage gradual replacement of antiquated data networking in favor of high performance TCP/IP networking that demands more rigorous cyber security controls and countermeasures. • It provides the industry time to evaluate and consider the impact of Smart Grid and NASPI on security controls/countermeasure needs prior to upgrading control systems networking. M) NEI encourages the team to reconsider the purpose of this standard as described above and believes the intent should be on identifying cyber vulnerabilities that could lead to High BES Impacts with appropriate H/M/L cyber asset controls based on the technology in use. A bright line of what will be considered High BES Impact threats should be the focus of Attachment 1. N) NEI does NOT support the work required in Attachment 2. The intended use of the information is not clear.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4 Informal Review

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the link below to submit comments on the proposed CIP-002-4. Comments must be submitted by **June 3, 2010.** If you have questions please contact Joe Bucciero at joe.bucciero@gmail.com or by telephone at (267) 981-5445.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Background Information:
FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards on Cyber Security. Some of the modifications were straightforward. Other Order 706 changes, such as modification to the scope of assets covered by the standard and consideration of the NIST framework, are more complex and required additional consideration. A Standards Drafting Team (SDT) was appointed by the Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. The SDT has been assigned the responsibility to review each of the CIP reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706.

Due to the large number of changes, some of which are complex issues, directed in Order 706 and the complexity of the project, the SDT adopted a multi-phase strategy to revise the CIP standards. The initial phase of the project modified the CIP standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706. The SDT's work in this initial phase resulted in Version 2 of the CIP standards. On September 30, 2009 FERC approved Version 2 of the CIP standards with an effective date of April 1, 2010.

In its September 30 Order, FERC directed NERC to make additional changes to two of the CIP standards (CIP-006-2 and CIP-008-2) and the associated implementation plan. Although FERC directed changes to only two of the eight (CIP-002-2 thru CIP-009-2) CIP standards, conforming changes were drafted for the remaining six CIP standards (CIP-002-2 through CIP-005-2, CIP-007-2, and CIP-009-2) to correct the cross references within the set of standards. The output of this work became Version 3 of the CIP standards. Version 3 of the CIP standards (CIP-002-3 to CIP-009-3) was approved by FERC on March 31, 2010 and become effective on October 1, 2010.

The SDT is currently developing changes to the CIP reliability standards to address the Order 706 directives that require significant industry debate.

In December 2009, the SDT posted an initial draft of the first CIP cyber security reliability standard (CIP-002-4 — Cyber Security — BES Cyber System Identification and Categorization) for a 45 day informal comment period. The SDT received more than 500 pages of comments from industry stakeholders. The SDT reviewed each of the comments received from the stakeholders, and considered their scope and direction throughout the development of the revised draft of the CIP standard. Subsequent to this initial posting, and in consideration of the significant change in scope for the revised CIP standard, the

drafting team has changed the designation of the first CIP reliability standard to CIP-010-1 — Cyber Security — BES Cyber System Categorization.

At its meeting on April 13–16, 2010, the SDT agreed on category headings for use in the posting and using a table approach for determining applicability. The SDT also agreed that, due to the nature of the proposed changes to the existing CIP standards, the best course of action would be to retire the existing standards and start a new sequence, starting with CIP-010 for the BES Cyber Asset Categorization. The SDT agreed to go forward with one standard (CIP-011) for all of the control requirements for the informal posting, asking for industry input on the comment form on the two format approaches considered.

In response to comments received from a large number of entities to post the requirements for categorization of BES Cyber Systems together with the requirements for the application of controls, the SDT has modified its schedule and intends to ballot the CIP standards as a single package. In consideration of the very different approach, model and format used in the drafting of these new CIP standards, the SDT is proposing a set of two standards in lieu of the original eight standards in the CIP series: CIP-010-1 establishes the foundation for cyber security protection by requiring the identification of what to protect and their categorization; CIP-011-1 establishes baseline cyber security requirements, which must be applied to protect the BES Cyber Systems identified and categorized in CIP 010-1 according their impact category. The alternate format would include CIP-010-1 as described above but would group the baseline cyber security requirements in multiple separate standards numbered consecutively as CIP-011-1, CIP-012-1, CIP-013-1, and so on. In the drafting these standards, the SDT considered CIP standards Version 1, 2, and 3 directives from FERC Order 706, FERC approved Interpretations to the CIP Version 1 requirements, and other cyber security standards such as NIST 800-53 and the DHS Catalog of Control Systems Security.

Implementation Plan Considerations

The SDT is currently developing an Implementation Plan for these standards which will consider the following:

1. BES Cyber Systems categorized as High Impact which were previously designated as Critical Cyber Assets;
2. BES Cyber Systems categorized as High Impact which were NOT previously designated as Critical Cyber Assets;
3. BES Cyber Systems categorized as Medium Impact which were previously designated as Critical Cyber Assets;
4. BES Cyber Systems categorized as Medium Impact which were NOT previously designated as Critical Cyber Assets;
5. BES Cyber Systems categorized as Low Impact which were previously designated as Critical Cyber Assets;
6. BES Cyber Systems categorized as Low Impact which were NOT previously designated as Critical Cyber Assets;
7. New requirements not previously included in the CIP Version 1,2, and 3 standards, as they relate to the above categories;
8. Re-categorized BES Cyber Systems;
9. Nuclear Facilities.

The Implementation Plan will be posted as part of the future posting package for formal comments.

The Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial draft of CIP-010-1 — Cyber Security — BES Cyber System Categorization and of CIP-011-1 — Cyber Security — BES Cyber System Protection. In addition, the SDT is requesting feedback from the industry on whether they prefer the currently proposed format for CIP-011-1, which contains a complete set of requirements; or an alternate format, where the requirements are grouped in separate standards. Industry feedback gathered will be utilized by the drafting team to refine the draft standard for formal industry review in July/August 2010.

***Please use the electronic comment form to submit your final responses to NERC.**

Questions:

1. Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.

   1.a. BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

   1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

   - Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
   - Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
   - BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
   - Alarm monitoring and processing specific to operation and restoration function, or
   - Coordination of BES restoration activities.

   ☐ Agree with proposed definition

   ☐ Disagree with proposed definition

   Comments:

2. The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree with scope

☐ Disagree with scope

Comments:

3. Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

4. Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

5. Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:

   3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

   3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

   3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

   Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

6. CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.

   Comments:

Questions — CIP-011-1 — Cyber Security — BES BES Cyber System Protection:
CIP-011-1 is a combination of CIP-003-3 through CIP-009-3 plus additional requirements based on FERC Order 706. The drafting team is proposing to retire the existing CIP-003-3 through CIP-009-3 standards once CIP-011-1 is adopted. This is the first time that CIP-011-1 has been posted for informal industry comment.

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?

   ☐ Keep CIP-011-1 as one document

   ☐ Break CIP-011-1 up into multiple standards

   ☐ No preference

   Comments:

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

    ☐ Agree

    ☐ Disagree

    Comments:

Security Governance and Policy (R1)

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

    ☐ Agree

    ☐ Disagree

    Comments:

Personnel Training, Awareness, and Risk Assessment (R2 – R4)

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

    ☐ Agree

    ☐ Disagree

    Comments:

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Physical Security (R5 – R6)

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

    ☐ Agree

    ☐ Disagree

    Comments:

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Electronic Access Control (R7 – R14)

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of

electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

☐ Agree

☐ Disagree

Comments:

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

☐ Agree

☐ Disagree

Comments:

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

☐ Agree with proposed method

☐ Combine Access Control requirements

Comments:

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

☐ Agree

☐ Disagree

Comments:

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

☐ Agree

☐ Disagree

Comments:

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each

Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

☐ Agree

☐ Disagree

Comments:

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

☐ Agree

☐ Disagree

Comments:

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

☐ Agree

☐ Disagree

Comments:

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

☐ Agree

☐ Disagree

Comments:

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

☐ Agree

☐ Disagree

Comments:

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

System Security (R15 – R19)

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Boundary Protection (R20 – R22)

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Configuration Change Management (R23)

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Information Protection and Media Sanitization (R24 – R25)

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

BES Cyber System Maintenance (R26)

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

    ☐ Agree

    ☐ Disagree

    Comments:

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

Cyber Security Incident Response (R27 – R29)

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

BES Cyber System Recovery (R30 – R32)

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

    ☐ Agree

    ☐ Disagree

    Comments:

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

    ☐ Agree

    ☐ Disagree

    Comments:

General Questions

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

    Comments:

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

    Comments:

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008)
2. Revised SAR and response to comments approved by SC (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009)
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)
9. Version 4 of CIP-002 posted for informal comment (December 29, 2009)
10. Version 1 of CIP-010 and CIP-011 posted for informal comment (May 3, 2010)

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	7/26/2010
2. Conduct initial ballot.	8/30/2010
3. Post response to comments on initial ballot.	9/10/2010
4. Conduct Second Ballot	10/04/2010
5. Post response to comments on second ballot	10/29/2010
6. Conduct Third (recirculation) ballot.	11/08/2010
7. Submit standard to BOT for adoption.	12/10/2010
8. File standard with regulatory authorities.	12/24/2010

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

Physical Security Perimeter

Electronic Security Perimeter

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Protection

2. **Number:** CIP-011-1

3. **Purpose:** To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES.

4. **Applicability:**

   4.1. For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

   4.1.1 Reliability Coordinator

   4.1.2 Balancing Authority

   4.1.3 Interchange Coordinator

   4.1.4 Transmission Service Provider

   4.1.5 Transmission Owner

   4.1.6 Transmission Operator

   4.1.7 Generator Owner

   4.1.8 Generator Operator

   4.1.9 Load-Serving Entity

   4.1.10 Distribution Provider

   4.1.11 NERC

   4.1.12 Regional Entity

5. **Effective Date:** To be addressed as part of the implementation plan that is currently under development

B. Requirements

Security Governance and Policy (R1) 4
Personnel Training, Awareness, and Risk Assessment (R2 – R4) 5
Physical Security (R5 – R6) 7
Electronic Access Control (R7 – R14) 9
System Security (R15 – R19) 14
Boundary Protection (R20 – R22) 17
Configuration Change Management (R23) 19
Information Protection and Media Sanitization (R24 – R25) 21
BES Cyber System Maintenance (R26) 22
Cyber Security Incident Response (R27 – R29) 23
BES Cyber System Recovery (R30 – R32) 25

Security Governance and Policy (R1)

R1. Each Responsible Entity shall develop, implement, and annually review one or more formal, documented cyber security policies that addresses the following for its BES Cyber Systems:

- **1.1.** Applicability to organizational and third-party personnel;
- **1.2.** Security roles and responsibilities, including those responsible for authorizing access;
- **1.3.** Identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard;
- **1.4.** Personnel training, awareness, and risk assessment;
- **1.5.** Physical security;
- **1.6.** Electronic access control;
- **1.7.** System security;
- **1.8.** Boundary protection;
- **1.9.** Configuration change management;
- **1.10.** Information protection and media sanitization;
- **1.11.** BES Cyber System maintenance;
- **1.12.** Cyber Security Incident response;
- **1.13.** BES Cyber System recovery.

Personnel Training, Awareness, and Risk Assessment (R2 – R4)

R2. Each Responsible Entity shall provide all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly reinforcement in sound security practices under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems.

R3. Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access when specified in *CIP-011-1 Table R3 – Cyber Security Training*, except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.

> For the purpose of this standard, external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.
>
> For the purpose of this standard, routable protocol is defined as a communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another.
>
> For the purpose of this standard, non-routable protocol is defined as a communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another.

3.1. This cyber security training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems, and include, at a minimum, the following required items:

- The proper use of BES Cyber Systems
- Physical access controls to BES Cyber Systems
- Visitor control program
- The proper handling of BES Cyber Systems information and storage media
- Identification and reporting of a Cyber Security Incident

3.2. For personnel having specified electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems

3.3. For personnel having a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems

3.4. For personnel having a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures

3.5. This Responsible Entity shall maintain documentation that such cyber security training is conducted at least once every 12 months from the date of initial training, including the date the individual's training was completed.

CIP-011-1 Table R3 – Cyber Security Training				
	Cyber Security Training is Required Prior to Obtaining:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
3.1	Electronic access to BES Cyber Systems		Required	Required
3.2	Physical access to BES Cyber Systems with routable external connectivity			Required

R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access when called for in *CIP-011-1 Table R4 – Personnel Risk Assessment*, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response, to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.

4.1. This personnel risk assessment program shall at a minimum include:

- Identity verification via photographic identification documentation issued by a government agency (i.e. Federal, State or Provincial)
- A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.

4.2. Each Responsible Entity shall document the results of each personnel risk assessment.

4.3. Each Responsible Entity shall update each personnel risk assessment at least once every seven years after the initial personnel risk assessment.

CIP-011-1 Table R4 – Personal Risk Assessment				
	A Personal Risk Assessment is Required Prior to Obtaining:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
4.1	Electronic access to BES Cyber System		Required	Required
4.2	Physical access to BES Cyber Systems with routable external connectivity			Required

Physical Security (R5 – R6)

R5. Each Responsible Entity shall apply the criteria specified in *CIP-011-1 Table R5 – Physical Security for BES Cyber Systems* to prevent and/or detect unauthorized physical access to BES Cyber Systems.

CIP-011-1 Table R5 – Physical Security for BES Cyber Systems				
	Physical Security for BES Cyber Systems shall:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
5.1	Restrict physical access to areas protecting BES Cyber Systems.		Required for external connectivity only	Required
5.2	Monitor physical access to areas protecting BES Cyber Systems.			Required
5.3	Log physical access to areas protecting BES Cyber Systems. Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.			Required
5.4	Log (manual or automated) the entry and exit of visitors (individuals not authorized to have unescorted physical access), including the date and time, to and from the areas protecting BES Cyber Systems.			Required
5.5	Authorize unescorted physical access to areas protecting BES Cyber Systems			Required
5.6	Review authorized unescorted physical access rights to areas protecting BES Cyber Systems on a quarterly basis.			Required
5.7	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.			Required
5.8	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours.		Control Center only	Control Center only
5.9	Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours.		generation or Transmission Facility only	generation or Transmission Facility only
5.10	Require continuous escort access of visitors (individuals not authorized to have unescorted physical access) within areas protecting physical access to BES Cyber Systems			Required

CIP-011-1 Table R5 – Physical Security for BES Cyber Systems				
	Physical Security for BES Cyber Systems shall:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
5.11	Review any unauthorized physical access attempts and handle such physical access attempts in accordance with its incident response procedures			Required

R6. Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in *CIP-011-1 Table R6 – Physical Access Control Systems* to prevent and/or detect unauthorized physical access to BES Cyber Systems.

CIP-011-1 Table R6 – Physical Access Control Systems				
	Physical Security Plans shall Require:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
6.1	Restricting physical access to areas protecting physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3.		Required for routable connectivity only	Required
6.2	Monitoring physical access to areas protecting physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3.		Required for routable connectivity only	Required
6.3	Implementing a maintenance and testing program to ensure that all physical access control systems identified under Requirement R5, Part 5.1, 5.2, 5.3 function properly. The program must include testing and maintenance of all physical security mechanisms on a cycle no longer than three calendar years.		Required for routable connectivity only	Required

Electronic Access Control (R7 – R14)

R7. Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in *CIP-011-1 Table R7– Account Management Specifications* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R7 – Account Management Specifications				
	The Account Management Documentation Shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
7.1	Identification of account types, including individual, group, shared, guest, system and administrative accounts, in use for BES Cyber Systems	Required	Required	Required
7.2	Acceptable use of each identified account types	Required	Required	Required

R8. Each Responsible Entity shall apply the criteria specified in *CIP-011-1 Table R8 – Account Management Implementation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R8 – Account Management Implementation				
	Account Management shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
8.1	Establish and implement a process for authorizing the addition of account(s) and associated access privileges		Required	Required
8.2	Conduct a quarterly review and verification of accounts and associated access privileges			Required
8.3	Monitor the use of shared and guest/anonymous accounts			Required

R9. Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in *CIP-011-1 Table R9 – Access Revocation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R9 – Access Revocation				
	Revoke System Access Under the Following Conditions:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
9.1	For personnel terminated for cause.	Within 24 hours	Within 24 hours	Within 24 hours
9.2	For personnel who no longer require such access to Control Center BES Cyber Systems		Within 36 hours	Within 36 hours
9.3	For personnel who no longer require such access to Transmission BES Cyber Systems		Within 72 hours	Within 72 hours
9.4	For personnel who no longer require such access to generation BES Cyber Systems		Within 72 hours	Within 72 hours

R10. Each Responsible Entity shall implement the account management access control actions specified in *CIP-011-1 Table R10 – Account Access Control Specifications* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.

CIP-011-1 Table R10 – Account Access Control Specifications				
	Account Access Control Specifications Includes the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
10.1	Change default vendor passwords after installation	Required	Required	Required
10.2	Passwords must be changed at least once every 12 months,	Required	Required	Required
10.3	Implement a password scheme that has the following attributes:[1] Minimum of six characters	Required	Required	Required
10.4	Implement a password scheme that has at least two of the following four attributes:[1] Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)		Required	
10.5	Implement a password scheme that has at least three of the following four attributes: [1] Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)			Required
10.6	Require that authorized access permissions are the minimum necessary to perform work functions		Required	Required
10.7	Require explicit authorization of access to system and security administrative functions within the BES Cyber System			Required
10.8	Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions			Required

[1]If a device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support.

R11. Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall implement the requirements included in *CIP-011-1 Table R11 – Wireless and Remote Electronic Access Documentation* to ensure that no unauthorized access is allowed to its BES Cyber Systems.

> Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System.

CIP-011-1 Table R11 – Wireless and Remote Electronic Access Documentation				
	Wireless and Remote Electronic Access Documentation Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
11.1	Identify use restrictions for wireless technologies	Required	Required	Required
11.2	If remote access is used and/or implemented, document the allowed methods for remote access	Required for external connectivity only	Required for external connectivity only	Required for external connectivity only
11.3	If remote access is used and/or implemented, establish and implement a defined process for authorizing the establishment of remote access and associated remote access privileges	Required for external connectivity only	Required for external connectivity only	Required for external connectivity only

R12. Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in *CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management* to ensure that no unauthorized access is allowed to its BES Cyber System.

CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management				
	Wireless and Remote Electronic Access Management Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
12.1	If remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges			Required for external connectivity only

R13. Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria specified in *CIP-011-1 Table R13 – Remote Access Revocation* to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems

CIP-011-1 Table R13 – Remote Access Revocation				
	Revoke Remote Access Under the Specified Conditions in the Time Frame Identified:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
13.1	Revoke remote access to Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access.		36 hours for external connectivity only	1 hour for external connectivity only
13.2	Revoke remote access to Transmission substation BES Cyber Systems when job duties no longer require BES Cyber System remote access.		72 hours for external connectivity only	6 hours for external connectivity only
13.3	Revoke remote access to generation BES Cyber Systems when job duties no longer require BES Cyber System remote access.		72 hours for external connectivity only	4 hours for external connectivity only

R14. Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in *CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls* to ensure that no unauthorized access is allowed to its BES Cyber Systems.

CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls				
	Wireless and Remote Electronic Access Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
14.1	If remote access is used and/or implemented, include authentication controls	Required	Required	Required
14.2	If remote access is used and/or implemented, include multifactor authentication controls			Required
14.3	Deny access by default; specify explicit access permissions		Required	Required
14.4	Display an “appropriate use banner” on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.			Required

System Security (R15 – R19)

R15. Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in *CIP-011-1 Table R15 – Malicious Code* to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.

CIP-011-1 Table R15 – Malicious Code				
	Malicious Code Protections Shall Consist of Processes to Perform the Following	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
15.1	Limit propagation of malicious code.		Required	Required
15.2	Detect and respond to the introduction of malicious code.		Required	Required
15.3	Implement processes to test and update malicious code protections.		Required	Required

R16. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R16 – Security Patch Management* in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated.

CIP-011-1 Table R16 – Security Patch Management				
	Security Patch Management Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
16.1	Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems.		Required	Required
16.2	Development of an implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability.		Required	Required

R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R17 – System Hardening* in order to reduce the available attack surface of the BES Cyber System.

CIP-011-1 Table R17 – System Hardening				
	System Hardening Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
17.1	One or more processes to ensure that only network accessible ports and services used by each BES Cyber System Component required for normal and emergency operations are enabled. In the case where unused network accessible services and communication methods cannot be disabled, the Responsible Entity shall document and implement a mitigation plan.		Required for external connectivity only	Required for external connectivity only
17.2	Disable, or render unusable, externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components.			Required

R18. Each Responsible Entity shall document and implement processes incorporating the criteria specified in *CIP-011-1 Table R18 – Security Event Monitoring* to ensure that security events are known, logged, and responded to on BES Cyber Systems.

CIP-011-1 Table R18 – Security Event Monitoring				
	Security Event Monitoring Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
18.1	Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components.		Required	Required
18.2	Implement and document one or more security processes for continuous security monitoring that issue alerts for detected system events related to cyber security.		Required	Required
18.3	Maintain logs of system events related to cyber security within the specified time period.		90 calendar days	1 year
18.4	Review logs of system events related to cyber security and maintain records documenting review of logs within the following time periods.		30 calendar days	7 calendar days

R19. Each Responsible Entity shall implement the criteria specified in *CIP-011-1 Table R19 – Communications and Data Integrity* to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.

CIP-011-1 Table R19 – Communications and Data Integrity				
	Communications and Data Integrity Protection Shall Consist of the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
19.1	Validate data inbound to a BES Cyber System in a Control Center.			Required for external connectivity only
19.2	Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously.			Required for external connectivity only

Boundary Protection (R20 – R22)

R20. Each Responsible Entity shall document and implement processes that establish electronic access points that incorporate the criteria in *CIP-011-1 Table R20 – Electronic Boundary Protection* to define an electronic security perimeter thereby minimizing the risk of system intrusion.

Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).

	CIP-011-1 Table R20 – Electronic Boundary Protection			
	Electronic Boundary Protection Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
20.1	Document all communication paths that transmit and/or receive digital information external to each BES Cyber System.	Required	Required	Required
20.2	Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems and other devices that denies access by default and allows explicitly authorized communication.	Required	Required	Required
20.3	Document and implement access control at each electronic access point established in Part 20.2		Required	Required
20.4	Document and implement one or more processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point.		Required for external connectivity only	Required for external connectivity only
20.5	Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period.		48 hours for external connectivity only	12 hours for external connectivity only
20.6	Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period.			7 calendar days for external connectivity only

R21. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R21 – System Boundary Protection* to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components.

	CIP-011-1 Table R21 – System Boundary Protection			
	System Boundary Protection shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
21.1	Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide logical separation that prevents access between each system.		Required	Required
21.2	Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.	Required	Required	Required

R22. Each Responsible Entity shall implement the criteria specified in *CIP-011-1 Table R22 – Protective Cyber Systems* to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems.

	CIP-011-1 Table R22 – Protective Cyber Systems			
	Protective Cyber Systems shall:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
22.1	Have remote access restricted as specified in Requirement R14 – Wireless and Remote Electronic Access Controls.	Required	Required	Required
22.2	Implement processes and procedures as specified in Requirement R16 -Security Patch Management			Required
22.3	Implement processes and procedures as specified in Requirement R18 -Security Event Monitoring			Required
22.4	Be changed only by authorized personnel in accordance with Requirement R23 - Configuration Change Management		Required	Required

Configuration Change Management (R23)

R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R23 – Configuration Change Management* to prevent and detect unauthorized modifications to BES Cyber Systems.

CIP-011-1 Table R23 – Configuration Change Management				
	Configuration Change Management Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
23.1	Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.	Required		
23.2	Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components, physical location, software (including version), active ports and services, any patches, and any custom software/scripts.		Required	Required
23.3	Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed.	Required		
23.4	Authorize and document changes to the BES Cyber System that deviate from the existing baseline configuration and update the baseline configuration and other documentation as necessary within 30 days of the change being completed.		Required	Required
23.5	Assess potentially impacted cyber security controls to verify controls are not adversely affected following a change to the BES Cyber System that deviates from the existing baseline configuration.			Required

CIP-011-1 Table R23 – Configuration Change Management				
	Configuration Change Management Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
23.6	For each change that deviates from the existing baseline configuration: • test the changes to the BES Cyber System in a test environment that closely models the software versions, active ports and services, any patches, and any custom software/scripts included in the baseline configuration of the BES Cyber System to ensure that cyber security controls are not adversely affected; • document the results of the testing and the differences between the test environment and the baseline configuration of the production environment including a description of the measures used to account for any differences in operation between the test and production environments as a result of the baseline divergence.			Required for Control Center only
23.7	Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes.			Required

Information Protection and Media Sanitization (R24 – R25)

R24. Each Responsible Entity shall document and implement one or more processes that incorporate the criteria in *CIP-011-1 Table R24 – Information Protection* to prevent unauthorized access to sensitive information associated with BES Cyber Systems.

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

CIP-011-1 Table R24 – Information Protection				
	Information Protection Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
24.1	Identify and classify sensitive information commensurate with its sensitivity and consequence as related to BES Cyber Systems.		Required	Required
24.2	Implement labeling and handling procedures for sensitive information according to its classification level.		Required	Required
24.3	Explicitly authorize personnel for access to sensitive information.		Required	Required
24.4	Revoke access to sensitive information within 24 hours for personnel terminated for cause.		Required	Required
24.5	Verify at least every 12 months that the access privileges to sensitive information reflect authorization.		Required	Required

R25. Each Responsible Entity shall document and implement one or more processes that incorporate the criteria in *CIP-011-1 Table R25 – Media Sanitization* in order to prevent the unauthorized dissemination of BES Cyber System information.

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

CIP-011-1 Table R25 – Media Sanitization				
	Media Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
25.1	Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.		Required	Required

BES Cyber System Maintenance (R26)

R26. Each Responsible Entity shall document and implement processes that incorporate the criteria in *CIP-011-1 Table R26– Maintenance* to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidently introduce malicious code into the BES Cyber System.

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

CIP-011-1 Table R26 – Maintenance				
	Maintenance Controls Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
26.1	Maintain a list of personnel authorized to perform maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.		Required	Required
26.2	Detect and prevent the introduction and propagation of malicious code on all maintenance devices.		Required	Required

Cyber Security Incident Response (R27 – R29)

R27. Each Responsible Entity shall document and implement one or more BES Cyber Security Incident response plans that incorporate the criteria in *CIP-011-1 Table R27 – Cyber Security Incident Response Plan Specifications* so that responses to Cyber Security Incidents involving BES Cyber Systems can occur.

CIP-011-1 Table R27 – Cyber Security Incident Response Plan Specifications				
	Cyber Security Incident Response Plan Specifications Shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
27.1	A process for classifying events as Cyber Security Incidents.	Required	Required	Required
27.2	Roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	Required	Required	Required
27.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) either directly or through an intermediary.	Required	Required	Required

R28. Each Responsible Entity shall test its BES Cyber Security Incident response plan(s) as specified in *CIP-011-1 Table R28 – Cyber Security Incident Response Plan Testing Specifications* to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System.

CIP-011-1 Table R28 – Cyber Security Incident Response Plan Testing Specifications				
	Cyber Security Incident Response Plan Testing Specifications Shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
28.1	Test the execution of the incident response plan (by responding to an actual incident, or with a paper drill, or with a full operational exercise) at least once every 12 months.		Required	Required

R29. Each Responsible Entity shall review, update and communicate its incident response plan(s) as specified in *CIP-011-1 Table R29 – Cyber Security Incident Response Plan Review, Update, and Communication Specifications* to ensure that the response plan(s) will function as intended and that personnel are aware of any relevant changes.

CIP-011-1 Table R29 – Cyber Security Incident Response Plan Review, Update, and Communication Specifications				
	Cyber Security Incident Response Plan Review, Update, and Communication Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
29.1	Review the incident response plan(s) at least once every 12 months	Required	Required	Required
29.2	Review the results of each incident response plan test or actual incident response within sixty calendar days of the execution, documenting any identified deficiencies or lessons learned associated with the response plan			Required
29.3	Update each incident response plan based on any documented plan deficiencies within thirty calendar days of the review of the execution of the incident response plan			Required
29.4	Update incident response plan(s) within thirty calendar days of any system, organizational, and technology changes that impact the response plan			Required
29.5	Communicate all updates to personnel responsible for the activation and implementation of the incident response plan(s) within thirty calendar days of the update being completed			Required

BES Cyber System Recovery (R30 – R32)

R30. Each Responsible Entity shall create, document, and implement recovery plan(s) for the disruption, compromise or failure of BES Cyber Systems that incorporates the criteria specified in *CIP-011-1 Table R30 – Recovery Plan Specifications* so that BES Cyber Systems can be restored to a defined state.

CIP-011-1 Table R30 – Recovery Plan Specifications				
	Recovery Plan Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
30.1	Conditions for activation of the recovery plan(s)		Required	Required
30.2	Roles and responsibilities of responders, including identification of the personnel responsible for recovery efforts		Required	Required
30.3	Required actions of personnel responsible for recovery efforts			Required
30.4	Processes for the backup, storage and protection of information required to successfully restore a BES Cyber System			Required
30.5	Processes for the restoration of BES Cyber Systems to include the following: • Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, • Load any information from the most recent, known secure backups, • Conduct a system test to verify functionality			Required

R31. Each Responsible Entity shall test its recovery plan(s) for BES Cyber Systems in accordance with the criteria specified in *CIP-011-1 Table R31 – Recovery Plan Testing Specifications* to verify recovery plan readiness and effectiveness.

CIP-011-1 Table R31 – Recovery Plan Testing Specifications				
	Recovery Plan Testing Specifications Shall Include the Following:	**Low Impact BES Cyber System**	**Medium Impact BES Cyber System**	**High Impact BES Cyber System**
31.1	Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months.		Required	
31.2	Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current.			Required
31.3	Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness			Required

R32. Each Responsible Entity shall review, update and communicate its recovery plan(s) in accordance with the criteria specified in *CIP-011-1 Table R32 – Recovery Plan Review, Update, and Communication Specifications* to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes.

CIP-011-1 Table R32 – Recovery Plan Review, Update, and Communication Specifications				
	Recovery Plan Review, Update, and Communication Specifications Shall Include the Following:	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
32.1	Review the recovery plan(s) at least once every 12 months or when BES Cyber Systems(s) are replaced, documenting any identified deficiencies		Required	Required
32.2	Review the results of each recovery plan test or actual incident recovery within sixty calendar days of the execution, documenting any identified deficiencies or lessons learned		Required	
32.3	Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the execution, documenting any identified deficiencies or lessons learned			Required
32.4	Update the recovery plan(s) based on any documented deficiencies, lessons learned or any system, organizational, and technology changes at least once every 12 months		Required	
32.5	Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review of the execution of the recovery plan			Required
32.6	Update recovery plan(s) within thirty calendar days of any system, organizational, and technology changes			Required
32.7	Communicate all recover plan updates to personnel responsible for the recovery plan efforts within thirty calendar days of the update being completed		Required	Required

C. Measures

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention (to be added)

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1			

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (March 20, 2008 – April 19, 2008)
2. Revised SAR and response to comments approved by SC (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by NERC Board of Trustees (May 6, 2009)
6. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 3 of CIP-002 to CIP-009 final ballot (December 14, 2009)
8. Version 3 of CIP-002 to CIP-009 approved by NERC Board of Trustees (December 16, 2009)
9. Version 4 of CIP-002 posted for informal comment (December 29, 2009)
10. Version 1 of CIP-010 and CIP-011 posted for informal comment (May 3, 2010)

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 45-day comment period and pre-ballot review.	7/26/2010
2. Conduct initial ballot.	8/30/2010
3. Post response to comments on initial ballot.	9/10/2010
4. Conduct Second Ballot	10/04/2010
5. Post response to comments on second ballot	10/29/2010
6. Conduct Third (recirculation) ballot.	11/08/2010
7. Submit standard to BOT for adoption.	12/10/2010
8. File standard with regulatory authorities.	12/24/2010

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

BES Cyber System Component – One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

BES Cyber System – One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Control Center – A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

- Critical Assets
- Critical Cyber Assets
- Cyber Assets

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-010-1

3. **Purpose:** To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.

4. **Applicability:**

4.1. Functional Entities:

For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Function**a**l Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

4.1.3. Interchange Coordinator

4.1.4. Transmission Service Provider

4.1.5. Transmission Owner

4.1.6. Transmission Operator

4.1.7. Generator Owner

4.1.8. Generator Operator

4.1.9. Load-Serving Entity

4.1.10. Distribution Provider

4.1.11. NERC

4.1.12. Regional Entity

4.2. **Physical Facilities**

4.2.1. All BES Facilities under NERC jurisdiction including those structures, components, equipment and systems of facilities within a nuclear generation plant not regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

5. **Effective Date:** To be addressed as part of the implementation plan that is currently under development

B. Requirements

R1. Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* to identify BES Cyber Systems for the application of security requirements. *(Violation Risk Factor: High)*

R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in *CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems* to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES. *(Violation Risk Factor: High)*

R3. To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall: *(Violation Risk Factor: High)*

3.1. Review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

3.2. Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

3.3. Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES.

C. Measures

M1. Each Responsible Entity shall have evidence identifying and documenting each of its BES Cyber Systems that execute or enable functions defined *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* as required in R1.

M2. Each Responsible Entity shall have evidence identifying the categorization of each of its BES Cyber Systems that execute or enable functions defined in *CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES* categorized in accordance with *CIP-010 – 1 Attachment II – Impact Categorization of BES Cyber Systems* as required in R2.

M3. Each Responsible Entity shall have evidence that it has reviewed its identification and categorization of its BES Cyber Systems and updated the applicable documentation within 45 calendar days of the completion of the review or the completion of such change to the BES.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1. Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2. ERO for Regional Entity.

1.1.3. Third-party monitor without vested interest in the outcome for NERC.

1.2. Data Retention

Each Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence for Requirements R1, R2 and R3, and Measures M1, M2 and M3 for a full calendar year or since the last audit, whichever is longer.

If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or as specified above, whichever is longer.

The Compliance Enforcement Authority, in conjunction with the Registered Entity, shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes

1.4.1 Compliance Audits

1.4.2 Self-Certifications

1.4.3 Spot Checking

1.4.4 Compliance Violation Investigations

1.4.5 Self-Reporting

1.4.6 Complaints

1.4. Additional Compliance Information

None

2. Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	5% or fewer BES Cyber Systems have not been identified.	More than 5% but less than or equal to 10% of BES Cyber Systems have not been identified.	More than 10% but less than or equal to 15% of BES Cyber Systems have not been identified.	More than 15% of BES Cyber Systems have not been identified.
R2	5% or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 5% but less than or equal to 10% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 10% but less than or equal to 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.	More than 15% of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category.
R3	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 45, but less than or equal to 60 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 60, but less than or equal to 70 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 70, but less than or equal to 80 calendar days of the completion of the change.	The Responsible Entity failed to update its documentation of BES Cyber Systems in accordance with Requirement R3 for more than 80 calendar days following the completion of the change.

E. Regional Variances

None.

Version History

Version	Date	Action	Change Tracking
1.000	5/3/2010	Initial draft of Version 1 posted for informal comment.	

CIP-010-1 — Attachment I

Functions Essential to Reliable Operation of the Bulk Electric System

The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes.

Dynamic Response — Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Balancing Load and Generation — Activities, actions and conditions for monitoring and controlling generation and load.

Controlling Frequency (Real Power) — Activities, actions and conditions to control frequency within defined bounds.

Controlling Voltage (Reactive Power) — Activities, actions and conditions to control voltage within defined bounds.

Managing Constraints — Activities, actions and conditions to maintain operation of BES elements within their design limits and constraints.

Monitoring & Control — Activities, actions and conditions that provide monitoring and control of BES elements.

Restoration of BES — Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Situational Awareness — Activities, actions and conditions to assess the current, expected, and anticipated state of the BES.

Inter-Entity Real-Time Coordination and Communication — Activities, actions and conditions for real-time coordination and communication between Responsible Entities' System Operators.

CIP-010-1 — Attachment II

Impact Categorization of BES Cyber Systems

1. High Impact Rating (H)

Each BES Cyber System that can affect operations for:

1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW.

1.2. Synchronous condensers, static VAR compensators and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.

1.3. Generation Facilities that are pre-designated as reliability "must run" assigned units that have Wide Area reliability impacts.

1.4. Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan.

1.5. Transmission Facilities with four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher in the Texas and Quebec Interconnections.

1.6. Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005.

1.7. Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). Where IROLs are not used or are not available, Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading.

1.8. Transmission Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated capabilities described in Part 1.1 above.

1.9. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities.

1.10. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have impact beyond the local area.

1.11. BES Elements that perform automatic aggregate load shedding of 300 MW or more.

1.12. Reliability Coordinator functions performed by primary or backup Control Centers.

1.13. Balancing Authority functions performed by primary or backup Control Centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 4,000 MW

or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections.

1.14. Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations operating at 300 kV or above in the Eastern and Western Interconnections or operating at 200 kV and above in Texas and Quebec Interconnections or functionality that remotely controls a BES Cyber System with a High Impact Rating.

2. Medium Impact Rating (M)

BES Cyber Systems that can affect operations for:

2.1. Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real Power capability of 1000 MW or more, not included in Section 1.

2.2. Synchronous condensers, static VAR compensators and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 500 MVAR or more, not included in Section 1.

2.3. Generation Facilities that are pre-designated as Reliability “must run” assigned units not identified in Part 1.3.

2.4. Transmission Facilities with four or more transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.

2.5. Transmission Facilities that if destroyed, degraded, misused or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated capabilities described in Part 2.1 above, not included in Section 1.

2.6. Transmission Facilities operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.

2.7. Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.

2.8. Balancing Authority functions performed by primary or backup Control Centers, of Transmission Facilities or generation Facilities, singularly or in combination, of 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.

3. Low Impact Rating (L)

All other documented BES Cyber Systems that can affect operations and are not categorized in Section 1 as having a High Impact Rating or in Section 2 as having a Medium Impact Rating.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Informal Comment Period Open
May 4–June 3, 2010

Now available at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Project 2008-06: Cyber Security Order 706 (Phase II)

As authorized by the Standards Committee, the Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial drafts of CIP-010-1 — Cyber Security — BES Cyber System Categorization and of CIP-011-1 — Cyber Security — BES Cyber System Protection **until 8 p.m. Eastern on June 3, 2010.**

In addition, the drafting team is requesting feedback from industry representatives on whether they prefer the currently proposed format for CIP-011-1, which contains a complete set of requirements; or an alternate format, where the requirements are grouped in separate standards. Industry feedback gathered will be utilized by the drafting team to refine the draft standard for formal industry review in July/August 2010.

Instructions

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Lauren Koller at Lauren.Koller@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Next Steps

Since this is an informal comment period, the drafting team will post the comments received and a summary of how the team used the comments. More information about the scheduling for this project is available in the comment form for this posting. The Standards Committee has authorized the deviations from the current standards development process, such as this informal comment period, to help the team meet its schedule for the delivery of the set of CIP standards.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy.

The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

At its meeting on April 13–16, 2010, the SDT agreed that, due to the nature of the proposed changes to the existing CIP standards, the best course of action would be to retire the existing standards and start a new sequence, starting with CIP-010 for the BES Cyber Asset Categorization. The SDT agreed to go forward with one standard (CIP-011) for all of the control requirements for the informal posting, asking for industry input on the comment form on the two format approaches considered.

In response to comments received from a large number of entities to post the requirements for categorization of BES Cyber Systems together with the requirements for the application of controls, the SDT has modified its schedule and intends to ballot the CIP cyber security reliability standards as a single package. In consideration of the very different approach, model, and format used in the drafting of these new CIP cyber security standards, the SDT is proposing a set of two standards in lieu of the original eight standards in the CIP Cyber Security series: CIP-010-1 establishes the foundation for cyber security protection by requiring the identification of what to protect and their categorization; CIP-011-1 establishes baseline cyber security requirements, which must be applied to protect the BES Cyber Systems identified and categorized in CIP 010-1 according their impact category. The alternate format would include CIP-010-1 as described above but would group the baseline cyber security requirements in multiple separate standards numbered consecutively as CIP-011-1, CIP-012-1, CIP-013-1, and so on.

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Coordinator
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
Distribution Provider
NERC
Regional Entity

Proposed Glossary of Terms Changes

New terms:

BES Cyber System Component
BES Cyber System
Control Center

Terms to be retired once the standards that use those terms are replaced:

Critical Assets
Critical Cyber Assets
Cyber Assets
Physical Security Perimeter
Electronic Security Perimeter

Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance,
please contact Lauren Koller at lauren.koller@nerc.net

Consideration of Comments on Question 7 from Informal Comment Period Conducted May 5 – June 4, 2010

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

(Note that information from Attachment II in CIP-010 was used to develop the 'bright line' criteria in Attachment 1 in CIP-002-4.)

Summary Consideration: The primary comments from Attachment II concerned the High Impact categorization of all generation Facilities designated as Blackstart Resources and Facilities required to support a primary Cranking Path. Commenters indicated that not all of the Blackstart resources or Cranking Paths identified in an Entity's restoration plan are material to the restoration of the BES, suggested creating the definition of the "Primary Cranking Path", and including Blackstart Resources and Cranking Path Facilities under multiple impact categories. Due to development of the interim CIP 002 4 asset identification standard, there is insufficient time for the development and approval of a "Primary Cranking Path" definition. A "Primary Cranking Path" definition may also be beyond the scope of this drafting team. They also expressed concern that categorizing all Blackstart Resources as High Impact may cause Entities to reconsider and reduce the number of units identified as Blackstart resources. This criterion designates only those generation Blackstart Resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan. The Cranking Path Facilities have been further refined to only include those Facilities required for initial switching, up to the point where multiple path options exist.

Entities responded that the criterion using the contingency reserve to categorize High Impact generation was confusing. The contingency reserve requirement varies, and may be significantly smaller value than 2000MW. The approach to use the contingency reserve requirement or a fixed threshold was discussed extensively by the team and industry volunteers. To simplify the criterion, a fixed numeric threshold will be used. Some commenters suggested that the categorization should also be based on the unit service factor or capacity factor. These factors are largely determined by market forces, and may not be suitable for addressing reliability issues.

Commenters disagreed with the term "must run". The term "must run" is not defined term in the Glossary of Terms Used in NERC Reliability Standards, has more relevance to the market function, and is not uniformly applied or understood in the electric industry. The term has been removed from the criterion.

Entities indicated that the Low Impact category was too broad, and included assets which have no impact on the BES. Respondents suggested a "None" category, a lower threshold below which the standards are not applicable, specific criteria for

categorizing Low Impact assets, or the allowance for an engineering assessment to determine impact. The intent of the drafting team is to develop appropriate minimal cyber security requirements for Low Impact assets.

Organization	Yes or No	Question 7 Comment
Platte River Power Authority		1.1 is confusing. Consider revising:For the preceding 12 months did the Generation Facility's net Real Power capability (rated net) exceeds the largest value of either the Contingency Reserve or the Reserve Sharing Group's total reserve sharing obligation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW. 2.7. "switching stations operated at 200kV or above" should read "switching stations operated between 200kV and 299kV"
National Rural Electric Cooperative Association (NRECA)		In 1.1, "must run" must be more clearly defined and there needs to be language to make clear how Generation Facilities are labeled "must run" -- i.e., who determines the "must run" status?In 1.5 and other places in this document, the term Transmission lines is used. What does "lines" mean? One wire? One three-phase circuit? One single phase of a three phase circuit? Please make this clear so there is no confusion for registered entities when determining High, Medium or Low.In 1.10, please provide an explanation of what "impact" and "local area" means in the phrase "have impact beyond the local area." Add language to 1.10 as needed to make this more clear.
Emerson Process Management		It is only uncertain how the criteria of 2000MW and 1000MW were chosen for generation facilities.
Arizona Public Service Company		These criteria are closely related to the definition of a BES Cyber System and the feedback for question #2. If the intent is to categorize the majority of BES Cyber Systems into the Low, Medium and High Impact Categories, with the current timeline specified in the definition of a BES Cyber System, it may lead Entities to exclude from Impact Categorization (by the Definition) Cyber System Components that the drafting team did not intend. A preferred approach may be to eliminate the time windows from the definition, causing all BES Cyber Systems to be inventoried, and enhancing the Impact Categories with additional time window criteria. For example, a High category may be further refined by specifying an impact window of 0-15 minutes, a Medium of 16-240 minutes, a Low of 241-1440 minutes (24 hours), etc. Additionally, a further Impact Category of 'None' may be beneficial if the 15-minute time windows is removed from the definition. This would allow a floor to be utilized in the Impact Categorization of 'Low' so that it would not result in unintended consequences of including undesired BES Cyber System Components in a category with Standard

Organization	Yes or No	Question 7 Comment
		applicability. Further comments regarding the (as-of-yet undefined) implementation schedule include concerns that a long implementation schedule or different implementation schedules for High, Medium and Low both raise the risk of confusion as well as the risk or FERC disapproval. An alternate method, in conjunction with the definition and Impact Category adjustments mentioned, of creating a phased implementation schedule, by time period (12 months, 24 months, 36 months, for example) would allow the applicable standards to increase over time for the lower categories. This would also allow for some Standards to be applied earlier than other Standards in the same Impact Category.
ISO New England Inc	No	“Must run” in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
Madison Gas and Electric Company	No	1.3 and 2.3 utilize the words “must run”. Must run is used in many markets whereby a GO may designate a unit to be online outside the need for reliable operations of the BES. Since “must run” is not defined, it is recommend that the SDT remove the term “must run”.
Progress Energy (non-Nuclear)	No	All T/D substation capacitor banks that provide system reactive support are controlled through a capacitor bank control program residing on the substation gateway device. However the DSCADA master may be included in 1.2 (more than 1000 MVAR). 2.4 will bring many T/T substations into consideration with the four or more lines >200kV. Also see comment 4.Attachment II defines "Each Cyber System that can affect operations for..." as it relates to Impact Rating on BES. For new combined cycle facilities which will include diverter dampers to allow simple cycle operation can we designate separate Cyber systems for simple cycle operation (approximately 70% of total plant output) and combined cycle operation (approximately 30% of total plant output). Potentially that would define each system as a "Low " impact versus a combined Medium to High. The plants are being designed to go from combined cycle to simple cycle operation in less than 15 minutes. We will need to know whether this designation is allowed and then design the cyber system(s) architectures appropriately.
Consultant	No	Attachment II - Section 1.1 & 1.2 To avoid confusion, suggest consistent wording in the parenthetical phrases following the words "singularly or in combination" in these sections.Section 1.2 - Similar to section 1.1, should there be a 12 month component to the Reactive Power criteria in addition to the 1,000 MVAR.Section 1.3 & 2.3 - The term "pre-designated" doesn't make sense. A facility is not in the "must run" status unless it is

Organization	Yes or No	Question 7 Comment
		"designated". Additionally, the statement has "must run" units both "designated" and "assigned", and semantically these are two different conditions.Section 1.3 & 2.3 - Further, the reliability "must run" status is an economic and contractual condition rather than a BES operational condition. It would seem that the plants that would be designated as reliability "must run" should have a BES operational or reliability criteria, independent of their "must run" status, which should be the criteria used to include or exclude these facilities.Section 1.6 - suggest including the title of EOP-005 in the statement as a complete reference citation.Section 1.9 - suggest including the title of NUC-001 in the statement as a complete reference citation.Section 1.10 - suggest clarifying which entity makes the determination that a RAS has "impact beyond the local area." - RAS Owner, RAS Operator, or appropriate regional entity.Section 1.11 (& throughout CIP-011) - BES Elements, BES elements, and elements are used throughout this standard. It is not clear if all are intended to be the glossary definition of 'Elements', or if 'BES elements' or 'BES Elements' are new definitions or incorrect application of the glossary term 'Elements'. Please clarify the usage.Sections 1.8, 1.13, 2.5 - These sections include the words "singularly or in combination" without a subsequent parenthetical qualifier. Suggest consistency with sections 1.1 & 1.2 as discussed above.Section 2.1 - See comments on sections 1.1 and 1.2 regarding consistency of parenthetical statement.Section 1.1, 1.3, 1.4, 1.5, 1.7, 2.1, etc. - Multiple sections use the terms Generation Facilities or Transmission Facilities with capitalization that should indicate a defined term, either by this standard or in the current glossary. These terms are not defined in the current glossary. Suggest consistency of using defined terms throughout the standard.Section 2.1 - The criteria in this section are not parallel to the criteria in section 1.1 with a 'downsized' value. The term "most current and prior to most current rated" is not defined, or included in the glossary. Suggest clarifying this section, and defining or referencing the terminology.
E.ON U.S.	No	CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 “High Impact Ratings” of the categorization of the BES Cyber Systems. E ON U.S. proposes that only Control Centers and Backup Control Centers fall into the High Impact Rating category. All other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category.More generally, “reliable operation” of the interconnected BES is defined in Section 215(a)(4) as:” . . . operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.”Attachment II’s low impact category appears completely untethered to the statutory definition of reliable operation of the bulk power system. Attachment II also appears to introduce an ill-defined set of multiple contingencies or sequence of events that needs more definition and boundaries to be of any practical use and to provide a reasonable means for compliance cost quantification.

Organization	Yes or No	Question 7 Comment
Kansas City Power & Light	No	Do not agree with several of the items listed in Attachment II. Items 1.7 & 1.8 are too broad. There are any number of combinations of transmission facilities that can be removed from service such that the undesirable effect of exceeding an IROL limit or the loss or reduction of generation would occur. Recommend their removal as the remaining items left in Attachment II are sufficient to capture the HIGH impact areas. Item 1.10 regarding SPS is too broad. SPS systems are in place for a number of different reasons, including the protection of facilities from damage. The SPS that should be considered here are only the SPS that are intended to prevent cascading, uncontrolled separation, or instability.Item 1.14 is too broad and would include facilities that are unnecessary. Recommend tying Control Centers in where facilities are identified in 1.5. Recommend the following language for consideration: Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations for transmission facilities identified by 1.5.
FirstEnergy Corporation	No	FE suggests that item 1.5 be removed such that it is effectively reclassified as a medium impact and covered by item 2.4. Within the High Impact category, items 1.6, 1.7 and 1.8 appropriately cover those situations where Transmission Facilities should rise to a High Impact level.Consider removing item 1.9. This delves into a nuclear plant safety concern that is covered by the NUC-001 standard and not directly associated with BES reliability. If in item 1.1 a 2000MW level adequately depicts a High Impact generation facility hurdle then transmission facilities associated with a 900MW nuclear plant should not be deemed High Impact for BES reliability.In item 1.10 the term “local area” is vague and open to interpretation. Its suggested to simplify such that all SPS and RAS systems would be treated as High Impact. If the intent is to exclude SPS or RAS associated with limiting generation output under contingency loss of certain Transmission Facilities then consider a separate Medium Impact SPS or RAS describing those instances and rewrite 1.10 to say “Special Protection Schemes, Remedial Action Schemes (RAS) or automated switching of BES elements not include in Section 2, item 2.x” However, the preference is to keep it simple and just treat all SPS and RAS items as High Impact.Suggest adding thresholds below which no measures need to be taken. The low impact rating as written could require significant effort for negligible security and reliability improvement.
National Grid	No	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue. National Grid recommends a tabular format similar to the tables in CIP-011-1 with various criteria listed under Low Impact, Medium Impact, and High Impact. This will help in understanding the key differences among the three categories efficiently.”Must run” in 1.3 and 2.3 is a phase should not be used, even if quotations are around it,

Organization	Yes or No	Question 7 Comment
		because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
Green Country Energy	No	No comment
American Electric Power	No	Overall we like the concept of these gradients, but need more time to fully ascertain the validity of the breakpoints. It is uncertain what engineering analysis drove these specific categorization levels. We assume that there could be a significant difference from region to region, and the SDT should consider regional impacts for the categorization.
Regulatory Compliance	No	Qualifier should include capacity factors averaged over the last five years - otherwise it will require some large plants that are only on-line several days a year to remediate to the "High Impact" category
Manitoba Hydro	No	Regarding criterion 1.1, the phrase “with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW” is difficult to understand. For some utilities, the required reserve obligations could be a small value which would not compare very well to the proposed 2000 MW limit for utilities with NO reserve obligations (such as small utilities). A related minimum value for utilities with reserve obligations should be provided, or the greater value of the required reserve obligations and 2000 MW should be used .Regarding criteria 1.5 and 2.4, clarify the requirements through the appropriate use of colons, semi-colons and numbers. It is not clear as drafted whether phrase “with four or more transmission lines” applies to Texas and Quebec.
Seattle City Light	No	see prior comments
Indeck Energy Services, Inc	No	The system of 3 categories oversimplifies the BES. 1) The grouping of, for example, all generators of capacity less than 1,000 MW (except for special cases like Must Run units) as LOW needs to be further subdivided. The categorization ignores the Functions in Attachment I. Not all generators have the same impact on the BES ALR for all functions. Different types of generators have different effects on the BES ALR. This isn’t to say that all generators should not be categorized, but not all require the same LOW level of requirements. Choosing only 3 categories was highly arbitrary. The LOW category should be subdivided into 3 or more groups reflecting the relative impact on BES ALR that was used to differentiate the HIGH and MEDIUM groups. 2) Additionally, the standards ignore the fact that access to BES cyber facilities can be

Organization	Yes or No	Question 7 Comment
		controlled at either end of a communications path. If it is adequately controlled at one end, then controlling the other end or the middle is less important, if not unimportant. For example, an RTU at a small generator that is a window to the BES cyber facilities at the control center is a bigger risk for BES ALR at the control center than it is at the generator. Any effect on the generator may be insignificant, whereas, access to the control center could be critical. Applying controls at the control center takes away the need to control all of the insignificant RTU's, but not the ones affecting other parts of the BES. 3) Nowhere in the categorization process is the potential impact on BES ALR assessed by Function. Attachment II makes arbitrary categories that may be appropriate for the HIGH and MEDIUM categories, but has not been done for the remainder that are lumped in the LOW category. The concept of impact to the BES ALR is missing from the categorization process. The impact on the BES ALR of, for example a 999 MW generator versus a 499 MW generator versus a 299 MW generator are very different and different by Function as well. The impact on the BES ALR should be assessed for all facilities in the LOW category to differentiate them. All of the facilities should be categorized as to the impact on the BES ALR by function. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, with various combinations of facility types and functions from Attachment I.
Reliability & Compliance Group	No	These criteria do now however, exclude many systems that were previously identified as CCA's. However they also include many systems that registered entities eliminated using the RBAM.
BCTC	No	This looked very thorough. Great job!
Xcel Energy	No	While the draft provides guidance in Attachment II as to which BES elements are classified as High, Medium, and Low impact, no criteria is provided for why each element was assigned into the specific impact category. The decision to place each element into a category is not based on any identified objective criteria. The SDT should publish the criteria used to place each item under the assigned category.
Alberta Electric System Operator	No	
American Municipal Power	No	
Black Hills Corporation	No	
ERCOT ISO	No	

Organization	Yes or No	Question 7 Comment
GE Energy	No	
Idaho Power Company	No	
LADWP	No	
Liberty Electric Power, LLC	No	
Michigan Public Power Agency	No	
Network & Security Technologies Inc	No	
Northeast Utilities System	No	
Old Dominion Electric Cooperative	No	
PNM Resources, Inc.	No	
Progress Energy - Nuclear Generation	No	
SPS Consulting Group Inc.	No	
Tenaska	No	
The United Illuminating Co	No	
Western Area Power Administration	No	
CWLP Electric Transmission,	Yes	

Organization	Yes or No	Question 7 Comment
Distribution and Operations Department		
Independent Electricity System Operator	Yes	(1) We support explicitly including Restoration of BES as a critical function. However, in the proposed standard it is limited to blackstart generation and transmission subsystem cranking paths (impact level H, items 1.4 and 1.6 in Attachment II). The impact criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). With these criteria, in Ontario we would drop 6 generating stations (a total of over 3000 MW capacity) from a High impact (current Critical Assets) to a Low impact category. We suggest to add a requirement in the High category for generation essential to facilitate restoration as determined by the RC.(2) 1.3 "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (3) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice.(4) 1.13: BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then simply say so. (5) 2.3: See our comments on 1.3. We do not see the need for this category.(6) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
IRC Standards Review Committee	Yes	(i) There are "bright-line" cutoffs for the range of violations for MW of generation (1.1, 2.1) and voltage levels (1.5, 2.4). Although these cutoffs are appropriate for most of the Interconnection(s), there may be local configurations that warrant that BES Cyber System to be rated other than what is defined with the "bright-line" cutoff. CIP-010-1 should either allow for a documented alternative rating or waivers be allowed to diverge from the cutoff limits.(ii) 1.3: "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service".(iii) 1.7: Violating IROL does not result in instability,

Organization	Yes or No	Question 7 Comment
		uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice.(iv) 1.13: A BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then simply say so.(v) 2.3: See our comments on 1.3. We do not see the need for this category.(vi) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
FEUS	Yes	*1.1; clarify 'if the Generation Facilities capability exceeds the largest value of the Contingency Reserve or reserve sharing obligations for the Reserve Sharing Group' the Contingency Reserve is also relative to the Reserve Sharing Group. *1.10: The drafting team should consider allowing for voltage differentiations for High and Medium SPS, RAS, or automated switching stations similar to that used in 1.5 and 1.14
Hydro One	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.We strongly suggest that a fourth category of NO IMPACT is included as follows: No Impact contains all other documented BES Cyber Systems that have no affect on operation and are not categorized as having either High, Medium or Low Impact rating.
Northeast Power Coordinating Council	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.

Organization	Yes or No	Question 7 Comment
Florida Municipal Power Agency	Yes	1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: “Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Net Winter Real Power capabilities of generators are to be used in determining the supply side of determining the mismatch. The greater of actual coincident peak load, or forecasted peak load for the next year, of the Reliability Coordinator is to be used for the demand side of the equation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, the supply-demand mismatch metric shall be equal to the largest loss of source plus 50% of the next largest loss of source for the Reliability Coordinator area.”Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets.Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:”Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area.” In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact”Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL.”Radial Facilities serving only load should not be included in 1.5 or 2.4. The term “Facilities” in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for

Organization	Yes or No	Question 7 Comment
		multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. FMPA suggests:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load Elements since those Elements are not Facilities.2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects.Black start and cranking paths should not be High Impact at all. High impact would be the system going black, a delay in restoring the system is a Medium Impact since the damage has already been done. Hence, 1.4 and 1.6 should be combined and made a Medium Impact.1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 2.4, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 2.4, or functionality that remotely controls a BES Cyber System with a High Impact Rating."
Southwest Power Pool Regional Entity	Yes	1.1: The criteria to include as High only the generation that exceeds the Contingency Reserve or reserve sharing obligation effectively removes nearly all generation resources from this impact category. 1.3: "Wide Area reliability impacts" as defined by the NERC Glossary of Terms (April 20, 2010) may be far too broad. If the unit is designated as RMR, it should be High impact regardless of the wide area consideration. 1.10: Please define the term "local area." 1.12 and 1.13: The Reliability Coordinator, and in the instance of a consolidated Balancing Authority, the Balancing Authority functions afforded a High impact categorization are fed real-time operational data from smaller, lower impact BES Cyber Systems owned and operated by other entities. Because of the criticality of the Reliability Coordinator and Consolidated Balancing Authority's near total reliance upon external real-time data sources, those sources need to also be afforded a High impact category. In particular, these BES Cyber Systems would include the EMS/SCADA and ICCP subsystems found in an entity's control center. 2.1: The 1000 MW criteria defining a Medium Impact generation asset will likely place most generation into a Low Impact category.
Oncor Electric Delivery LLC	Yes	1.10 needs to better define "local area" (eg. 3 busses) Need criteria for "Low" such that "None" is the lowest level of protection required. Also, there is a need to have categories for systems with no IP communication or dial-up only communications.
LCEC	Yes	2.4 Replace transmission facilities with "Substations and/or switching stations and two or more non-radial transmission lines". or"Transmission Facilities with four or more non-radial transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec

Organization	Yes or No	Question 7 Comment
		Interconnections, not included in Section 1.”2.7 change to "non-radial" Transmission substations or switching stations or”Primary or Backup Control Centers that remotely control two or more Transmission substations or switching stations, each with four or more non-radial transmission lines, operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.”
Turlock Irrigation District	Yes	Attachement II criterion #1.4 states that BES Cyber Systems that can affect operations for Blackstart Resources in the Transmission Operator's restoration plan shall be categorized as High Impact. This should be changed to include only the Blackstart Resources in a region's Blackstart Capability Plan because Transmission Operator's restoration plans typically include Blackstart Resources that are not material to the restoration of the BES. Blackstart Resources that are material to the restoration of the BES are designated by each Regional Entity in accordance with NERC Standard EOP-007-0 titled "Establish, Maintain, and Document a Regional Blackstart Capability Plan". We suggest that the wording of criterion #1.4 be changed to "Generation Facilities designated as Blackstart Resources in the Regional Blackstart Capability Plan". Making this change would maintain consistency between the Standards and would also be consistent with the Purpose section of CIP-010-1 which states that the categorization of BES Cyber Systems should be "commensurate with the adverse impact... on the reliability of the BES.Attachment II criterion #1.6 uses the term "primary Cranking Path". What is the meaning of the word "primary" as used in this context? We suggest that the wording be changed to "Facilities required to support Cranking Path(s) that are material to the restoration of the BES as used in a Transmission Operator's restoration plan per EOP-005".
Garland Power and Light	Yes	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line.General CommentNeed to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
Powersouth Energy Cooperative	Yes	CIP-010 Attachment II1.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered High Impact if singularly or in combination exceed 2,000 MW. It seems to be reasonable to apply the 2,000 MW limit to reserves as well with reserve requirements only greater than 2,000 MW being considered as High Impact. 1.4 Additional consideration should be given to categorizing

Organization	Yes or No	Question 7 Comment
		blackstart units in all cases as High Impact. Some units, while identified in a TO's restoration plan, are not part of the Regional Entities Restoration Plan. Some generation that may be used in a restoration effort may be removed from the TO's restoration plan to avoid implementation of High Impact security requirements. Some "middle ground" should be found so that more units can remain available in a restoration plan without being subject to costly security requirements and subsequently an increase in exposure for a utility to be non-compliant. It is recognized that there must be a sufficient number of blackstart critical units that remain protected by High Impact status to ensure restoration following an event. 1.10 Is "local area" meant to be the Balancing area or can the entity define local area.2.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered Medium Impact if singularly or in combination exceed 1,000 MW. It seems to be reasonable to apply the 1,000 MW limit to reserves as well with reserve requirements only greater than 1,000 MW being considered as Medium Impact. 3. Some consideration should be given to providing exclusions to exempt assets that in reality have no material impact.
City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
MidAmerican Energy Company	Yes	Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load".Subsequently, CIP-010-1 Attachment II item 1.4 should be updated to only designate Generation Facilities associated with the "Primary Cranking Path". ALSOMr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical asset systems that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Four critical units at MEC would move to low. Simultaneous loss of the four MEC units would impact the reliability of the BES. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
PacifiCorp	Yes	Comments: Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary

Organization	Yes or No	Question 7 Comment
		Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load".ALSO"Wide Area" impacts need to be clarified in Item 1.3 for "Must Run" units. ALSOMr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical assets that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Concerning generation facility capability, "rated net Real Power" can produce fictitious numbers that will never be attained. This should be the historical or commissioning test maximum net Real Power continuous output, whichever is greater.Wide Area is a very large area for WECC, as WECC is the RC. We are not sure if there are any generation facilities in WECC that have an impact on the whole of WECC. We are also not sure if generation being "pre-designated as reliability 'must run'" is a practice in all areas. It is possible that some units may be designated using other terminology or have detailed contracts. It may be better to remove the quotes and define Must Run Generation in the Glossary.Not all generation that is designated by the Transmission Operator's restoration plan as Blackstart is critical to the plan. It may be listed as a possible resource, but not a primary first choice. Further, much of the restoration plans are out of date and due for revision; requiring generation owners and operators to upgrade for CIP compliance only to have their plant removed in the new restoration plan in the next year or so would be wasteful. The purpose of a Blackstart resource in an old (pre-mandatory reliability standard compliance) restoration plan may be for local level of service resource for the TOP's local distribution area rather than a resource for BES reliability, i.e. the old plans to not coordinate well with each other. Last of all, should there not be a rating qualifier?
Detroit Edison	Yes	Criteria 1.3 and 2.3 should be removed for the following reasons:1. The term "reliability must run" is not defined.2. There is no generator that is so essential to reliability that it would need to run 100% of the time. 3. A generator could be required to run on a given day to serve load in an area that cannot be otherwise served due to a transmission constraint. This would be a temporary condition and should not warrant a high or medium classification.
Cogeneration Association of California and Energy Producers & Users Coalition	Yes	Criteria 2.4 should be clarified. The criteria states "Transmission Facilities with four or more transmission lines operated at 200kV or above..." Do two transmission lines, each with two circuits that can operate independently for a total of four circuits, count as two transmission lines or four transmission lines?
Exelon Corporation	Yes	Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment. A specific example is

Organization	Yes or No	Question 7 Comment
		the 4 or more Transmission line requirement. The previous draft had a 3 or more Transmission line requirement, so what was the basis for the 3 or more and, moreover, what is the basis for now changing it to 4 or more? The technical basis for generation limits in Attachment II is not provided. That is, the basis for the 2000 MW and 1000 MW thresholds appear arbitrary. Combined losses of greater than these values have occurred without significant impact to the BES. No “reasonable bounds” are allowed. For example, if a common vendor provides a cyber product in multiple generating stations, it appears that the assumption is that this common product, no matter how local its impact, creates a common mode failure for all plants simultaneously, resulting in the determination before the fact that this product will be rated as High Impact. No allowance is made for geographical location. For example, if a common cyber system is used in several large generating stations in different regions of the country, their simultaneous loss may result in no significant impact to the BES. However the deterministic MWe thresholds and simple “in combination” wording will result in virtually all such cyber systems rated as high, deterring use of common vendors, standardization, and economies of scale. Although moving to a more deterministic approach can be seen as increasing consistency in application of the standard, it would appear that a deterministic approach will decrease the flexibility of operation now allowed and may in fact, reduce BES reliability. As a modification to the Attachment, Exelon suggests that the existing deterministic criteria could be used, unless an entity chooses to show by actual historical data or modeling that such losses do not result in significant impact on the BES. This performance-based criteria could be expanded to define high, medium, and low impacts on the BES in terms of stability, voltage swing, etc.
American Transmission Company	Yes	For R1.4, we propose changing text from “designated as Blackstart Resources” to “designated as the primary Blackstart Resources” (similar to primary Cranking Path in 1.6). Add “restoration plan per EOP-005” (similar to 1.6). Note that Transmission Operators can only designate Blackstart Resources that have been volunteered to them by Generation Owners. All GO may choose not to volunteer any Blackstart Resources if they don’t want their associated cyber systems to be subject to this standard.For R1.10, we propose removing SPS from the criteria. SPSs cannot be approved by the Regional Entities unless they have been designed not to be critical to the BES (e.g., not critical if they operate when they should not or do not operate when they should).
SCE&G	Yes	How does the SDT see AGC coming into play in 1.1? Would every generator operated on AGC (if the aggregated total met the contigency reserve committment) be considered high impact, or just the centalized AGC itself?"Must Run" units needs to be clarified. Who determines if a unit is "must run"?1.4 This language needs to be clarified to identify resources designated as "Primary" Blackstart resources.1.5 Transmission lines should be change to Transmission Lines to utilize the NERC Definition1.8 Is this misusing/destroying one Transmission Facility at a time? SDT should consider defining "Transmission Facility" as a whole instead of utilizing seperate NERC Definitions for "Transmission" and "Facility"

Organization	Yes or No	Question 7 Comment
Entergy	Yes	If "size" of an electric facility remains the primary key differentiator for applicability of CIP requirements, which Entergy does not support, the following should be considered:1. High Impact Rating (H)"Each BES Cyber System that can affect operations for:1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities , singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW."Attachment II of CIP-010-1 qualifier 1.1 as stated above includes those generation facilities that have the capability to exceed the Contingency Reserve as High Impact to the BES. This is not truly indicative of the impact to the reliability to the BES. Entergy has multiple generation facilities with the capability to exceed the contingency reserve. However, their Service Hours (SH) are less than 900 hours and a Service Factor (SF) is less than 1.0, averaged over the past five years, where: - Definitions from GADS Data Reporting Instructions - January 2010- Service Hours - SH is the sum of all Unit Service Hours.- Period Hours - PH is the number of hours in the period being reported that the unit was in the active state.- Service Factor - SF = SH/PH x 100% Entergy proposes that a better representation for how much a generation plant runs, and therewith potential adverse impact on BES reliability, would be better determined by a measurement of the percent of SH, e.g., running at least 80% of the year; SH greater than 7008 hours per year, or, a SF of greater than 80% per year. Therefore, suggested alternative language for 1.1 is:"Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability), whose Service Factor (Service Factor = Service Hours per Year / Hours per Year X 100%) is equal or greater than 80% for a five year average."Additionally, extending this logic to the Medium Impact BES Cyber Systems, Entergy suggests replacement of language concerning Medium Impact Rating (M) 2.1 from: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real Power capability of 1000 MW or more, not included in Section 1."To: "Generation Facilities, singularly or in combinations (if using a shared BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability) with equal to or greater than 70% for a five year average."
Edison Mission Marketing and Trading	Yes	If we are going to use the High, Medium, and Low and there is not going to be a does not apply category, then there should be an engineering analysis or study performed by the BA's, RC's or an independent firm and it should include which sites/generators are critical and which are not and why. Once completed then and only then do we begin categorizing them into whatever scale the Standard Drafting Team and the included entities agree upon. As it is stands now we not only have to include nominal size generators, but wind sites as

Organization	Yes or No	Question 7 Comment
		well.
Puget Sound Energy	Yes	In 1.6, the restoration plan is linked to EOP-005, shouldn't the restoration plan mentioned in 1.4 be linked to EOP-005 as well?It appears that all BES Cyber Systems must fall into one of three categories. Are there any other criteria that would all for something not to be catorized as one of these three (i.e., such as non-dispatchable wind generation)?Also Blackstart should only classify as high those needed for primary region wide restoration since some (such as ours) are more secondary paths and there should be some minimum level of generation to be classified low. There is no need to classify as low a 20 MW hydro generator that does not impact BES reliability. We would recommend 300 MW.
Alliant Energy	Yes	In Article 1.3 we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.Article 1.4 - By including "All Black-Start Units" the standard is utilizing a "one-size-fits-all" strategy that the industry has recognized does not work for everything, and is working to address. All Black-Start units do not carry the same importance and this should be recognized in the standard. This philosophy may be counter-productive to system reliability as one classification may reduce the number of Black Start units that would be made available to a TOP's restoration plan due to the high initial security cost and the future possible financial risk of strict compliance guidelines with penalties.There should be a recognized hierarchy for the Black-Start resources, similar to the High, Medium, and Low for BES Cyber Systems. This methodology would assure Black Start units could be categorized by attributes in general to support the BES during a blackstart event. Each Balancing Authority Area (BAA) could be required to have a minimum number of high priority Black Start units depending on the BAA size to support the area during a black out. Lower priority units would be used for stabilizing power at generating stations, local area islanded load and used as a backup plan if all other contingency plans would fail.Article 1.6 - This item should reflect the same categorizing as is recommended in the comment to Article 1.4 above.Article 2.1 - Please clarify "with aggregate higher of the most current and prior to most current rated net Real Power capability." We believe it would be clearer if stated as below: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System) with a rated Real Power capability of 1000 MW or more, not included in Section 1."Article 2.3 - we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.
Public Service Enterprise Group companies	Yes	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6 requires that only the "primary cranking path" transmission facilities need to be categorized with a "High Impact Rating". Statement 1.6 implies that

Organization	Yes or No	Question 7 Comment
		some Blackstart Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
ReliabilityFirst Staff	Yes	In Part 1.1, the referent for “largest value” does not seem to be appropriate. Suggest changing the wording to “average value.” In Part 1.4, a “Blackstart Resource” is only the first resource that starts in a system restoration. Suggest changing the wording to “Generation Facilities required to support the Cranking Path(s) identified in Part 1.6.” In Part 1.6, a “primary” Cranking Path is not required to be identified in an entity’s restoration plan by EOP-005. Suggest changing the wording to “Facilities required to support at least one Cranking Path.” In Part 1.10 “local area” should be defined. As we are not certain what is meant by this term, we have no suggested wording.
RRI Energy	Yes	Include or add a "No impact category" that is determined by the RC.
MRO's NERC Standards Review Subcommittee	Yes	Item 1.3We believe this item may be problematic in nature, as the designation of reliability “must run” units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc.Item 1.4Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact.To implement this approach, we believe it is imperative to consider the Blackstart Resource’s actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8:”Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.”We believe this approach should provide a better sense of a facility’s true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.Item 1.5We need to clarify the meaning of “Transmission lines”. If a 300 kV substation has a terminal connected to a

Organization	Yes or No	Question 7 Comment
		345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line.We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher..."Item 1.6We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.Item 1.14We would recommend rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System.Item 2.7We would recommend rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System.Section 2 AdditionsWe would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
Minnesota Power	Yes	Item 1.4:Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. In theory, on a smaller scale, this appears to be a "one size fits all" approach, but in reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, Minnesota Power believes that there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact.To implement this approach, Minnesota Power believes it is

Organization	Yes or No	Question 7 Comment
		imperative to consider the Blackstart Resource's actual role in the restoration plan, not just the fact that it has been included. For example, a 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, Minnesota Power proposes that the Standards Drafting Team allow Registered Entities to assess the relative importance of a Blackstart Resource based on the importance of the facilities it directly supports.Minnesota Power recommends rewording item 1.4 as follows utilizing the existing language of Item 1.8:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."Minnesota Power believes this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.Item 1.14:Minnesota Power recommends rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System.Item 2.7:Minnesota Power recommends rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, which are not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System.Section 2 Additions:Minnesota Power recommends adding the following items under section 2, Medium Impact Rating, for consistency with the proposed Item 1.4:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
The Empire District Electric Company	Yes	Item 1.4Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same "one size fits all" approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. A regional study performed by the regional entities would be an excellent approach to determine this.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports

Organization	Yes or No	Question 7 Comment
		restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports.We would recommend rewording item #1.4 as follows, leveraging the existing language of Item #1.8:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."Since item #1.6 is also related to system restoration, we would recommend rewording it as follows for consistency in approach: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We would also recommend adding the following items under section 2, Medium Impact Rating: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.Item 1.5We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line.We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply changing the High Impact criteria to mirror that of the Medium Impact (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher...".
Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS), which address the current structure of Attachment II as proposed. However, LES believes a better overall approach would be applying Engineering studies to truly determine a facility's impact on the Bulk Electric System. We realize an Engineering study is not as simple as a "bright line" based metric. Unfortunately, the Bulk Electric System is not a simple system - it is actually very complex. So in order to properly assess the importance of the various facilities that make it up, LES feels a complex Engineering study is required.
Luminant	Yes	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ...

Organization	Yes or No	Question 7 Comment
Nuclear Energy Institute	Yes	Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW?
NextEra Energy Corporate Compliance	Yes	NextEra finds that a catch-all for Low impact is a fatal flaw. There should be some threshold that is justified for low. For example, a proper minimum criteria for LOW impact BES Cyber Systems could be:Cyber Systems that control BES level facilities that meet one of the following: 1) three or more transmission circuits operated at 100 kV or above not covered in Section 1 or 2, 2) two or more transmission circuits and two or more autotransformer with a secondary voltage 100kV or above,3) two or more transmission circuits and generation capacity at the site of greater than 1000MWAlternatively, a NO IMPACT category may be added which eliminates subjectivity in which BES Cyber components need to be reviewed. Single point buses representing looped load serving type stations cannot produce results worse than single contingency which must be operated to at all times. An additional item that should be specifically covered is the use of remote access for transmission and / or generation control locations and their applicability to the High, Medium, Low and/or No impact criteria.The term "affect operations" can be subjective and can be open to interpretation. NextEra suggests changing the15 minute requirement to “in real time (instantaneous). For example, closed loop control, which does not allow time for human intervention.”NextEra also recommends adding the word “both” prior to monitor and control.NextEra would also like to know what does 1.1.1 of section D mean? This is unclear. A suggestion would be eliminating or providing a specific definition.
Pacific Gas & Electric Company	Yes	Not all blackstart resources should necessarily be considered high impact. Suggest revising 1.4 as follows:Generation Facilities designated as Blackstart Resources and explicitly listed as essential to the restoration of the BES in the Transmission Operator’s restoration plan.
Northeast Utilities	Yes	NU is concerned with some of the impact criteria in Attachment II related to generation facilities. To base impact on “bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows. Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause levels of impact to the BES.
Matrikon Inc.	Yes	Please describe how the 15-minute time horizon would fit into Attachment 2. Is the intent for the 15-minute

Organization	Yes or No	Question 7 Comment
		horizon to provide a level of realism to determination of impact? To bring in more BES Cyber systems that could have indirect impact, or an escape clause if effects don't occur within 15 minutes?
USACE HQ	Yes	Please read answer to question 4.
BGE	Yes	Provide additional clarification of "automatic aggregate". For instance, does automatic mean an application that is kicked off without human intervention or does automatic mean after an operator hits a button? Suggest adding the word "instantaneous" before load shedding to clarify.Additional clarification on 1.14 (What is meant by "functions")
Southwestern Power Administration	Yes	Rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity, a better approach may be to include performance/results-based criteria in Attachment II.However, if the current approach is forwarded, I would suggest the following improvements:1.4. Generation Facilities designated as Primary Blackstart Resources in the entity's restoration plan. 1.7 Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs).1.10 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that if destroyed, degraded, or misused, would violate one or more Interconnection Reliability Operating Limits (IROLs).1.11. Delete. Is this not a Control Center issue?1.12. Control Centers that perform the Reliability Coordinator functions. 1.13. Control Centers that perform the Balancing Authority functions for 4,000 MW or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections. 1.14. Control Centers that perform the Transmission Operator functions for a Facility with a High Impact Rating. 2.4. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more System Operating Limits (SOLs)2.7. Control Centers that perform the Transmission Operator for a Facility with a Medium Impact Rating, not included in Section 1. 2.8. Control Centers that perform the Balancing Authority functions for 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.
Southern California Edison Company	Yes	SCE believes Attachment II should be modified to account for only the capacity that can be controlled by qualifying systems. As currently written, Attachment II defines the amount of generation under control as the rated capacity of the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to

Organization	Yes or No	Question 7 Comment
		attachment II, this would then categorize as “high impact rating”. However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000 respectively. This would place the system in a “low impact rating” according to the attachment. For that reason, SCE believes that Attachment II should be modified to account for only the capacity that can be controlled by the system.
San Diego Gas and Electric Co.	Yes	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have “BES outage” or reliability implications but may not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole.
Constellation Energy Control and Dispatch, LLC	Yes	See answer to Question 4.
Constellation Energy Commodities Group Inc.	Yes	See answer to Question 4. Please clarify the intended treatment of a Generation Management System (“GMS”). Attachment II implies that capacity monitored by a GMS system would be aggregated to determine its impact categorization. However, to be consistent with the intention to protect connections that truly impact the BES net real power capability should only be aggregated within a balancing authority.
MWDSC	Yes	See comments for question 4 above.
Wolverine Power	Yes	See comments listed for 1.a
Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment II would work.Also, for 1.1, either increase the net MW rating or add an annual capacity factor to a generating unit to account for old units at a site that no longer run because no longer economical. These types of facilities should not have to meet High category requirements if they no longer run. Also, for 1.3 add more detail. Explain pre-designated. Assigned by who? Explain Wide Area reliability impacts.
WECC	Yes	Similar to our previous comment, if Attachment 1 is expanded to include in scope reliability coordination functions critical to reliable operation of the BES outside of 15 minutes the impact levels need to be updated. While many functions of a Reliability Coordinator are critical and should be an high impact, not all functions of reliability coordination should be made high impact. For instance, Coordinated Outage systems while important to the reliability of the BES and should be in scope, should best be classified as a low-impact BES Cyber System.The considerations for identification and categorization has been elevated to a high level such that BES Cyber Systems and not individual devices are identified based on their specific functionality. It is suggested that if BES Cyber Systems are to be indentified and categorized there be some inclusion and

Organization	Yes or No	Question 7 Comment
		development of a process to granulate these systems down to their individual component level.Further, the quantitative qualification bar has been set to level that precludes most BES Cyber Systems from reaching identification as a high or even medium level of impact. Taking into account. If a BES Cyber System can impact reliability a baseline set of security controls should be established that creates tracking for all assets, accountability for access to these assets, and physical and electronic protection for these assets.Specific Line Item Comments(1.1) The standard, as drafted, seemingly excludes all generation but large dams, large mine-based coal plant and nuclear plants?(1.1) The developed sentence structure lends itself to multiple interpretations and will prove to be difficult to audit consistently. (1.1) Is the term aggregated defined as geographically co-located, common substation, common communication paths, etc?(1.6) What about redundant paths? There is no requirement to identify and document multiple paths. (1.6) A reference to EOP-008 would also be appropriate.
Con Edison of New York	Yes	Specific comments on the Categorization:The impact categories should be linked to the reliability Standard functions in Attachment I. Therefore, the High, Medium and Low ratings should reference specific Standards whenever possible. o 1.1: This requirement should be broken down into two requirements. One should refer to BAL-002 and reserves needed to be compliant. The second should be any generation facility with a common BES Cyber System greater than 2,000 MW. o 1.2: This should be linked to the function of "controlling voltages". Two other concerns; first - shunt reactors and capacitors are not included and second - there needs to be a technical basis for a Reactive Power capability limit. o 1.3: Suggest moving to "Low" category since reliability must run equipment is frequently a local congestion or voltage control situation. This would not qualify for a "High" impact rating. o 1.4: Black start resources should only be designated as a High Impact Rating if they are the only resource in the TOP's restoration plan. If the TOP has multiple restoration resources and procedures, the resources should be a Medium Impact Rating. Reference this to EOP standards. o 1.5: OK o 1.6: This item should be included in item 1.4 o 1.7: FACTS devices are used to control voltage and power flow. o 1.8: This should be included in requirement 1.1 o 1.9: OK o 1.10: Refer to PRC standards o 1.11: A basis for the 300 MW or greater UFLS system should be provided. o 1.12, 1.13, and 1.14 address Control Centers and should be aggregated into one requirement based on RC functions, BA functions, TOP functions and TO functions. In addition, there may be a conflict between a Control Centers with a "Low Impact Rating" and a single substation with a "High Impact Rating". The DT should consider addressing this conflict where the "BES Cyber Security Components" on one side of a device (e.g. breakers) is a "high impact" while the command signal will be a "low impact" device. General comment on criteria for categorization:Overall, the high, medium, and low levels do not properly meet the needs of the BES. The DT should be looking at what the system does and determining its ability to impact the BES rating rather then the impacted equipment. For example, SCADA systems should be High whether they are on the 138 kV or 345 kV. Wide scale damage can be done with access to the SCADA system, however only local issues can occur with access into a single non-networked microprocessor relay. Alarm panels and

Organization	Yes or No	Question 7 Comment
		other microprocessor that do not have direct impact should also be at lower level. Items that set levels should be a medium level. Basis for criteria for categorization is needed:Attachment II to CIP-010 contains a number of what appear to be administratively determined “bright lines.” Please provide both the detailed rational supporting each “bright line” and a specific quantification of the reliability benefits resulting from its implementation. In responding to this question, please focus more on the technical, reliability-related rational and improvements for each “bright line” selected, rather than on the source of any particular number. Reference any white papers, studies, expert opinion, or other documentation relied upon and supporting the “bright lines” selected.For example, in Attachment II category High Impact for item 1.11, please explain why 300 MW was selected. We are not so much interested in any reference to a 300 MW EOP-004 DOE reporting requirement, as we are in the specific criticality of the 300 MW level to BES reliability, e.g., 300 MW represents a large (>10%) percent of area load, or in the case of inadvertent actuation would cause an uncontrolled system instability(ies) and cascading, or in the event of a failure-to-actuate would cause the Interconnection UFLS program not to return frequency to nominal within the program required time period. What if for a given entity 300 MWs is not a significant percentage of local load, or inadvertent actuation would not cause uncontrolled instability and cascading, or failure-to-actuate would not prevent the return of frequency to normal within the required time period? Why rate such aggregate automatic load shedding “High” rather than “Medium” or “Low?” Are there any Interconnection-wide studies which would support this 300MW “bright line” value? Please provide any reference(s).
Allegheny Energy Supply	Yes	Suggested revision for 1.2:Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.
Allegheny Power	Yes	Suggested revision for 1.2:Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to

Organization	Yes or No	Question 7 Comment
		restoration of the BES.Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”.Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of termsThe Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.Under Frequency Load Shed systems under a common control system.
EEI	Yes	Suggested revision for 1.2:Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. As a result, the drafting team should consider whether to combine Items 1.4 and 1.6. Moreover, most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from providing additional protections for more valuable facilities. Moreover, this may create incentives for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES.It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration.EEI suggests the following definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”.In addition, the drafting team should modify the wording to only include units designated on a seasonal or annual basis. Regarding 1.7, EEI recommends striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of termsSuggest Adding:1.15 Control Centers including Generation Control Centers.Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.EEI suggests that 1.11 in Attachment II be revised as follows:”BES Elements that perform automatic aggregate load shedding of 300 MW or more under a common control system.”]

Organization	Yes or No	Question 7 Comment
APPA Task Force	Yes	The APPA Task Force commends the drafting team on their work on CIP-010-1. We appreciate the team's consideration of our Task Force comments from the previous informal comment period. We feel it is especially important for entities to have the option of categorizing the impact level based on the Contingency Reserve or total of reserve sharing obligations as stated in 1.1. However, we are concerned with the "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc. These thresholds do not have a basis from industry experience and could be challenged by entities or regulators. We are concerned that having chosen these numbers without empirical data supporting them, the numbers can easily be changed without the supporting empirical data. It is our recommendation that these numbers be evaluated more closely. At a minimum, the thresholds should be quantified to show what percentage of generation and transmission facilities would be designated under each Impact Rating. Florida Municipal Power Association (FMPA) provided some suggested alternative calculation methods for the Impact Categorization of Attachment II. We provide them here for the drafting team's discussion in evaluating the bright line thresholds.FMPA Comments:Categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: o High (has the potential to cause an Adverse Reliability Impact) o Medium (has the potential to require planned/controlled loss of load) o Low impact (has no potential to cause loss of load) Make changes to existing criteria: 1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets.Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second

Organization	Yes or No	Question 7 Comment
		largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:"Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact."Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL."Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. We suggest:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load since that those Elements are not Facilities.2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects.1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 1.5, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 1.5, or functionality that remotely controls a BES Cyber System with a High Impact Rating."End of FMPA comments.The APPA Task Force also supports the proposal by the MRO-NERC Standards Review Subcommittee (MRO-NSRS) in their comments on Item 1.4 and 1.6 to assign the impact rating of blackstart units and cranking path relative to assigned impact rating of the generating facilities it directly supports. We feel that inclusion of all blackstart resources in the High Impact Rating will waste limited resources protecting facilities which are not in support of High Impact generation.MRO-NSRS proposal:High Impact:1.4 "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."1.6 "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."Medium Impact:2.X "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."2.X "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation

Organization	Yes or No	Question 7 Comment
		Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1.”
US Bureau of Reclamation	Yes	The criteria defined in this and several previous requirements are based around BES Cyber Systems, which under the definition of BES (per the WECC Glossary) does not include all power system assets. Therefore, there appears to be a category of Cyber Assets that do not presently require any protection measures (i.e., they might control a powerplant feeding a radial load or be associated with a system of less that 100kV. The classification "Low" will potentially include those systems which do not have an impact. It is counterintuitive to classify a system as low when it has No Impact. The Team should develop a description of "Low" similar to that which was provided for "High" and "Medium". Then the Drafting Team could issue a statement that systems not classified as "High", "Medium" , or "Low" would be classified as "No Impact".
Dominion Resources Services, Inc.	Yes	The criteria for categorization of Low Impact systems is too broad and uses the terminology “can affect” which the SDT has appropriately recognized is ambiguous. The following alternate wording is proposed:”All other BES Cyber Systems not categorized as having a High or Medium Impact rating that are required for the reliable operation of the BES.”
Southern Company	Yes	The definition of “pre-designated as Reliability must run” in Attachment II, 1.3 is unclear and cannot be implemented with existing practices in some utilities. For utilities who designate units as must run on a day-ahead basis in some cases, a valuable practice, every unit in the fleet would have to be classified as high impact. The wording should be changed to only include units designated on a seasonal or annual basis. In addition, a definition of “must run” should be provided or referenced from elsewhere in NERC documentation.The wording in 1.3 also creates a new requirement that all “must run” units be classified as to whether they have Wide Area impact, which is not currently required.Are there actually any “must run” units (or any units, for that matter) that have Wide Area impact?Because Blackstart Resources are included in Cranking Paths, 1.4 is redundant in light of 1.6 and should be removed. Alternatively, 1.4 should be limited to primary Blackstart Resources to match 1.6.In 1.4, consideration should be given to reducing the impact level for situations where multiple Blackstart Resources are available.Universally search for “effect” and replace with “adverse effect”.In 1.6, replace “support” with “is part of”.In 1.7, delete the phrase "including Flexible AC Transmission Systems (FACTS). This is redundant as it is referenced again in the following sentence.
Constellation Power Source Generation	Yes	The final sentence in 1.1 needs to be rewritten, as it’s extremely confusing. A suggestion would be to simply add the 2,000 MW bright-line at the end of the first sentence. It would read “Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve, total of reserve sharing obligations for the Reserve Sharing Group, or 2000 MW (if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is

Organization	Yes or No	Question 7 Comment
		established).” Is it the intent of the SDT for the MOD10 data to be the data used in this criteria? If so, that data changes seasonally, so a seasonal review would be needed, especially for units who are on the thresholds of the high/medium/low criteria. A suggestion would be to use nameplate data as that is a fixed rating that will not change. 1.4 and 1.6 should be combined together, as they are referring to similar items. The combined High Impact Rating should read “Generation, Transmission, and other Facilities required to support a primary Cranking Path used in a Transmission Operator’s restoration plan per EOP-005.” However, 1.4 and 1.6, either combined or separate, still penalize generation entities that own numerous black start facilities within a single Balancing Authority’s footprint. Generation entities in the aforementioned situation have already invested a lot to ensure the reliability of the BES, but under CIP-010 they will be forced to invest even more. A suggestion would be for the TOP to designate a percentage of the black starts as High, and the rest as medium or low depending on their MW size. Another suggestion would be for the TOP to specifically designate certain black start units as high, and the rest are classified based on their MVA size, with the caveat that the TOP should not designate all black start units as high to avoid liability.
Dairyland Power Cooperative	Yes	The impact ranking for blackstart should be equivalent to the highest impact of all transmission and control center systems. If an entity has only low or medium impact systems other than blackstart, a high impact for blackstart is not appropriate. 1.2 and 2.2 specify 1000 MVAR and 500 MVAR, respectively for categorizing reactive power facilities. Since reactive power problems are localized in general, these numbers seem to be high. It is difficult to set global criteria on reactive power as it is network dependent. I would advise about 50% of the proposed level to be more conservative.
Duke Energy	Yes	The quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System instability, separation, or cascading failures.Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW? o CIP10-1.4: We have many small sites (hydro’s) listed in our Blackstart plan because they are available. They are not essential to our plan, but because they are available, we list them. Under this guidance, we would be required to include them as “High Impact”, when in reality they are ‘Low’. The wording should be revised to reflect that only those

Organization	Yes or No	Question 7 Comment
		sites “REQUIRED” for Blackstart be secured under 1.4 o CIP10-1.6: We need a defined and clear understanding of what is intended in the use of the term “Cranking Path” as it relates to CIP and EOP-005. What is being sought under this requirement? The term is loosely defined in the glossary, and how it is interpreted by the industry may vary greatly from how it is intended by regulators. o Under our current understanding of the term, we would see minimal increase in sites added to our “High” list. However if we impose a severe interpretation, we could see an exponential increase to our ‘High’ list. o CIP10-1.7 & 2.5: The word ‘Misuse’ should be removed or very strictly defined. It is too vague to have meaning. o CIP10-1.11: Need a clear and functional definition of ‘Element’ for the industry to understand the intent of the requirement. Current glossary definition is poor at best.Also, revise 2.6. as follows: Transmission Facilities operated at 300 kV or higher, which have 2 or more 300kV or above lines, in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.
Bonneville Power Administration	Yes	The sixth line in 1.1 begins with the words “Generation Facilities.” Generation Facilities is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Since this phrase is not used at the beginning of a sentence, it should be “generation Facilities.” There is the same problem at the beginning of the second line in 1.2. That should also be changed to be “generation Facilities.”The first line in 1.7 contains the phrase “Flexible AC Transmission Systems (FACTS).” That phrase is not defined in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Aren’t all capitalized terms used in Standards supposed to be defined? Or does FACTS have a generally accepted definition in the industry? CIP-010-1 - Attachment IIImpact Categorization of BES Cyber Systems High Implact Rating (H)Each BES Cyber System that can affect operations for:1.1. Generation Facilities, etc."can affect operations" does not relate to impact. We suggest it be reworded:"If the BES systems can change operation by the following amounts they will be in the HIGH CATEGORY:- Generation - 4,000 MW- trip or reduce output of "MUST RUN" generators to below their MUST RUN amount.- Transmission - de-energize at least 4 lines above 300 kV- MVAR support - change MVAR by 1,000 MVAR
US Army Corps of Engineers, Omaha Distirc	Yes	The word "affect" in the first sentence is somewhat ambiguious and does not fit the intent of all of the subsequent paragraphs(1.4 & 1.6) Paragraph 1.3 define wide area impacts. Paragraph 1.4 should be limited to BES Cyber Systems that are required to energize a Blackstart Resource listed in the TO's system restoration plan per the GO's written restoration plan. As written it appears to apply to any BES Cyber System that merely affects the Blackstart asset and that all BES at such a facility would be High Impact which could have a chilling effect on an entities willingness to provide Blackstart resources. Paragraph 1.6 should be limited to BES Cyber Systems required to operate or support equipment in the primary cranking path. Again this would appear to apply to all BES Cyber Systems at such a facility merely because the facility was part of the cranking path regardless of their impact on system restoration. Paragraph 1.10 define impact beyond the local area.

Organization	Yes or No	Question 7 Comment
Midwest ISO	Yes	There is no documentation for the justification of the selection of the various thresholds. Justification of these thresholds should be documented and defended.
SRW Cogeneration Limited Partnership	Yes	There needs to be a category for "no impact". We are a small Cogen plant that does not even sell firm power to the grid. In essense, we are a steam plant that happens to generate electricity. We have no "Critical Assets" as defined by CIP-002. There needs to be an equivalent level for that in CIP-010. If there needs to be a system study performed by the RC to support a "no impact" rating, that's fine. And if a facility is found to be "no impact", then that facility should be exempt from the majority of further CIP requirements, just like today where CIP-004 thru CIP-009 do not apply to facilities with no Critical Assets/Cyber Assets and only R2 of CIP-003 applies.
Covanta Energy	Yes	There still needs to be some allowance to fewer mandatory requirements associated with smaller generators.... those in the 20-50 MW range (which are unmonitored) who typically have to notify their TOP/BA that they are on the system or off the system (or reduced load if applicable).
Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
We Energies	Yes	We Energies agrees with EEI Suggested revision for 1.2:Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more.We Energies agrees with EEI comments Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, "primary Cranking Path" is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES.It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration.Proposed definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for initial system restoration".Regarding 1.7, we recommend striking "Flexible AC Transmission Systems (FACTS)" because it would be included within Transmission Facilities. Although capitalized, it does not

Organization	Yes or No	Question 7 Comment
		appear in the NERC Glossary of terms.We Energies agrees with EEI. Suggest Adding:1.15 Control Centers including Generation Control Centers.Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.Under Frequency Load Shed systems under a common control system.
Ameren	Yes	We generally agree with the criteria used to identify “High” impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as “Medium” impact, but should be classified as “Low” impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as “Low” impact, as they likely have little impact on the BES. The use of TPL performance standards would confirm that many of these facilities have a “Low” impact.For 1.1 the 4th sentence should be reworded to say "total obligations for the entire Reserve Sharing Group." 1.3 needs clarification of what a "reliability must run" unit is. Also, clarify 1.4 if it refers to the actual black start unit, or the entire plant in which the black start unit resides. Last, clarify 1.6 on what magnitude of support is required by the facility. Currently this could apply to any Transmission or Generation Sub-system in the path.Performance criteria, such as the loss of 300 MW of system load to qualify for “High” impact or 100 MW of system load to qualify for “Medium” impact, should also be applied to the EHV facilities identified in items 1.7 and 2.6.
GTC & GSOC	Yes	We recommend that Attachment II be organized to more clearly indicate which items apply to which type of assets. In the case of Control Centers, it appears the primary applicable item in the High Impact category are 1.12, 1.13 and 1.14, but several other items could be misconstrued to apply as well, which could lead to those control centers being inadvertently given a High designation.
CenterPoint Energy	Yes	While it appears the SDT put a lot of effort in the development of Attachment II, the criteria to be used is arbitrary, is too prescriptive, does not allow for studies or analysis to determine whether or not the loss, compromise, or mis-use of an identified facility would have an impact on the reliable operation of the BES and, in some cases, appears inconsistent. For example; 1.5 Transmission Facilities with four or more Transmission lines operated at 300kV of higher in the Eastern or Western Interconnections or operated at 200kV or higher in the Texas or Quebec Interconnections would require any and all facilities meeting this criteria to be categorized as High Impact without any basis for this rating. Determining a facility’s impact to an electric transmission system involves more analysis than counting the number of transmission lines operated at or above a threshold voltage level; 1.14 Transmission Operator functions is based on the number of substations a control center may be able to remotely control. The previous criterion, 1.13 Balancing Authority functions, is based on the mega-watt amount the Control Center operates. Neither offers a basis for either the

Organization	Yes or No	Question 7 Comment
		number of substations or the mega-watt amount under the operation of the Control Center. While CenterPoint Energy would find Attachment II useful as a guide or systems to be considered it is apparent the SDT meant this to be a requirement and therefore CenterPoint Energy does not agree with Attachment II and suggests it be deleted.
Verizon Business	Yes	1) Attachment II, Item 1.1 regarding Generation Facilities – Suggest removing any reference to "Contingency Reserve" or "Reserve Sharing Group." Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW should be included as a High Impact Rating. Reference to the "Contingency Reserve" (etc.) comments can result in incorrect or inconsistent declaration of a generation asset being a High or Medium impact. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? For the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. This and any other questions from FAQ for CIP-002 should be addressed in the standard.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

to ensure the reliability of the bulk power system

September, 2010

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

TABLE OF CONTENts

Disclaimer 3

Executive Summary 4

Introduction 5

Overall Application of Attachment 1 7

Generation 9

Transmission 12

Control Centers 15

Guidance on the Implementation Plan 16

Conclusion 19

Disclaimer

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

Executive Summary

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

Introduction

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

Overall Application of Attachment 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it is to leave some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity should document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Generation

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. This criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system. In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review

period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as required to run to ensure reliable operation of the BES are designated as Critical Assets. These Facilities are often designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, these units are typically designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where multiple path options exist as Critical Assets. This criterion is sourced from requirements

in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where multiple paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Since the purpose of Special Protection Systems and Remedial Action Schemes is to prevent disturbances that would result in excursions beyond IROLs, often in lieu of building additional Transmission Facilities, it is expected that all such systems and schemes will be designated as Critical Assets. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets.

  Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets or used to control generation greater than an aggregate of 1500 MW in a single Interconnection as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections.

  It must be noted that this part does not include the term “control systems” to avoid including those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document “Security Guideline for the Electric Sector: Identifying Critical Assets”.

Transmission

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies,Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

  It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES.

- Parts 1.8 and 1.9 include those Transmission Facilities that would violate IROLs if they were rendered unavailable or degraded. By definition, IROLs are those operating limits that, if exceeded, would have a Wide Area reliability impact.

- Part 1.10 designates those Transmission Facilities as Critical Assets that directly connect Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES

operation within IROLs. By IROL definition, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates those control systems as Critical Assets that are capable of performing automatic load shedding of 300 MW or more. These may include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. Control Systems that provide a "one-button push" capability of shedding 300 MW or more would also qualify as Critical Assets.

  300 MW is the reporting threshold for DOE EIA-417.

Control Centers

Parts 1.14 and 1.15 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for a single BES asset should be evaluated as part of BES asset (e.g., control room for a single generation plant or transmission substation). Part 1.15 has already been discussed in the Generation section.

Part 1.14 designates all control centers and control systems used to perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA) or Transmission Operator (TOP). EOP-008 requires that RCs, BAs and TOPs "ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable." While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets, control systems at other applicable Responsible Entities that are used to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include control systems at Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. Control systems were specifically called out separately from control centers to ensure that Entities fully evaluate those systems used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. These control systems may be located at a data center that is not co-located with the control center itself.

.

Guidance on the Implementation Plan

In general, Responsible Entities must:

(1) Comply with CIP-002-4 on the Effective Date[3]

(2) Comply with CIP-003-4 through CIP-009-4 on the Effective Date for previously identified CCAs and

(3) Comply with CIP-003-4 through CIP-009-4 18 months after the Effective Date for any new Critical Cyber Assets identified as a result of Attachment 1 Criteria

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*, and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. Responsible Entities should then refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* if directed to in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard. Compliance milestones for CIP-003-4 through CIP-009-4 is determined based on specific cases outlined in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4.* These cases include the following:

- Critical Cyber Assets Already in Compliance with CIP-003-3 through CIP-009-3

  Since only conforming changes to CIP-003-3 through CIP-009-3 were made and no changes were made to the existing requirement language itself, those Critical Cyber Assets already in compliance with CIP-003-3 through CIP-009-3 should be compliant with CIP-003-4 through CIP-009-4 on the Effective Date of the Version 4 Standard.

[3] "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)." For example, if FERC approves CIP-002-4 on March 31, 2011, then US entities must be able to demonstrate compliance by October 1, 2011.

- Critical Cyber Assets at Critical Assets Newly Identified by CIP-002-4

  The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one time implementation window was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-003-4 through CIP-009-4. Since updates to the Critical Asset list must be made as necessary and since these updates may occur before the next scheduled annual review of the Critical Asset list as defined in CIP-002-4 R1, this implementation window is defined as a rolling window for the first 12-month period following the effective date of CIP-002-4.

  This rolling implementation window is only applicable to those Entities that have already defined Critical Cyber Assets according to previous versions of CIP-002. Since these Entities already have fully developed CIP programs, the implementation window for these newly identified Critical Cyber Assets is 18 months. This implementation window is shorter than the 24-month implementation period given to Entities that do not currently have existing Critical Cyber Assets as per the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.*

  This special implementation window is slightly modified for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the *Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.*

- All Other Critical Cyber Assets

  The compliance milestones for all other circumstances should be derived from the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* The modifications made to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* over the previous version of this plan were only those needed to conform to the Version 4 Standards.

The process for determining the compliance milestones for CIP-003-4 through CIP-009-4 is illustrated in the timeline and flowchart below.

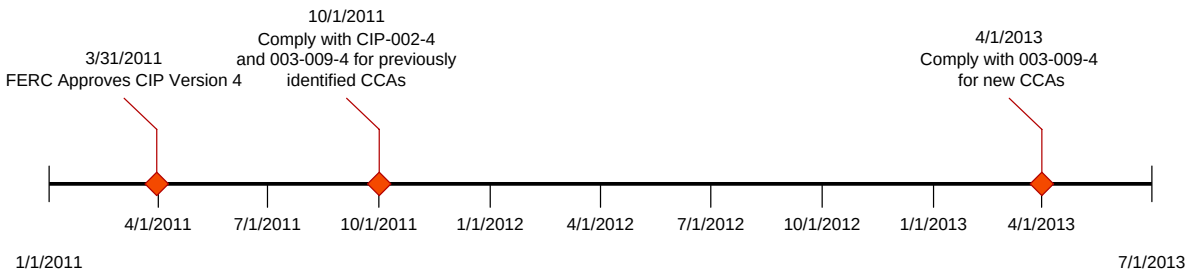
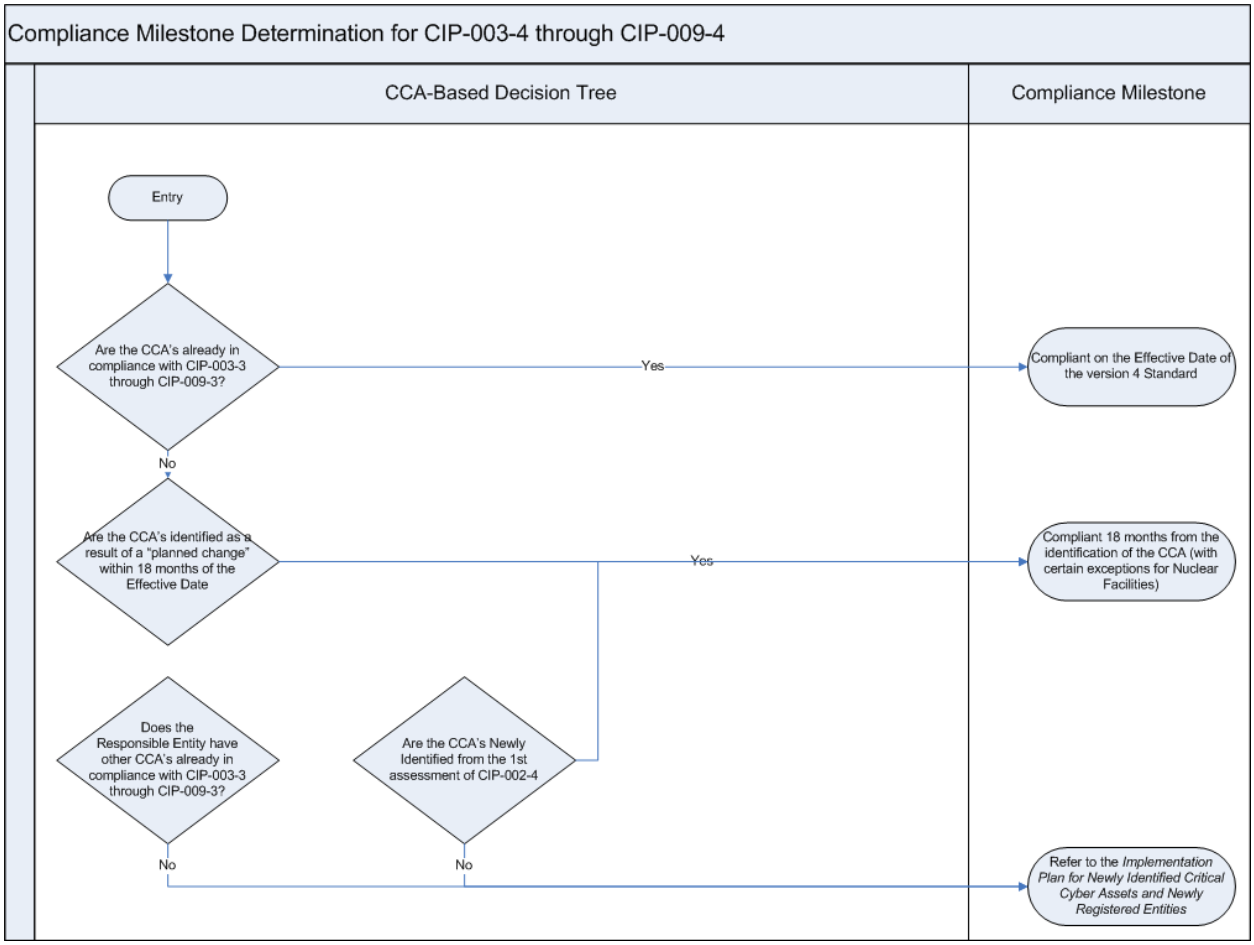


Figure 1: Sample Implementation Plan Timeline (General Case)



Conclusion

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.

VRF and VSL Analysis for Version 4 CIP Standards

This analysis applies to the following standards in the set of Version 4 CIP standards

- CIP–002–4 — Cyber Security — Critical Cyber Asset Identification
- CIP–003–4 — Cyber Security — Security Management Controls
- CIP–004–4 — Cyber Security — Personnel and Training
- *CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)*[1]
- CIP–006–4 — Cyber Security — Physical Security
- CIP–007–4 — Cyber Security — Systems Security Management
- CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
- CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

VRF Analysis

The proposed VRFs are based on previously approved VRFs for CIP-002 with conforming changes (R1 eliminated, R2 – R4 changed to R1 – R3).

No changes are proposed for the VRFs previously approved for CIP-003 through CIP-009.

VSL Analysis

The proposed VSLs are based on the previously approved VSLs for CIP-002 with conforming changes (R1 eliminated, R2 – R4 changed to R1 – R3). CIP Version 2 and CIP Version 3 VSLs are the same as CIP Version 1 VSLs, but CIP Version 2 and Version 3 VSLs have not been approved by FERC.

No changes are proposed for the VSLs previously approved for CIP-003 through CIP-009.

[1] CIP-005-4 is being processed as an Urgent Action revision under Project 2010-15 and includes modifications to one of the requirements. The conforming changes identified to update cross references to the correct version of CIP standards within CIP-003 through CIP-009 will be applied to CIP-005-4 after it has completed its balloting through the Urgent Action process.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mapping Document Showing Translation of CIP-002-3 – Cyber Security — Critical Cyber Asset Identification into CIP-002-4

Standard: CIP-002-4		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Requirements in CIP-002-4 (Comments)**
R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets. R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria. R1.2. The risk-based assessment shall consider the following assets: R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard. R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System. R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.	Replaced with a determined criteria list in CIP-004-2 - Attachment 1	The risk-based Critical Asset assessment methodology is being replaced with a determined criteria list in Attachment 1 in response to FERC Order 706 paragraph 236 and paragraph 253. *236. Pursuant to section 215 of the FPA, the Commission approves Standard CIP-002-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop modifications to Standard CIP-002-1. The required modifications are discussed below in the following topics regarding CIP-002-1: (1) need for ERO guidance regarding the risk-based assessment methodology; (2) scope of critical assets and critical cyber assets; (3) internal, management, approval of the riskbased assessment; (4) external review of critical assets identification; and (5) interdependency analysis.* *253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion*

Standard: CIP-002-4		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Requirements in CIP-002-4 (Comments)**
R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.		*whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.*
R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	Replaces risk-based assessment methodology with a determined criteria list in CIP-002-4 - Attachment 1. Renumbered as R1.	Proposed CIP-002-4 Requirement R1: R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria.* The Responsible Entity shall review this list at least annually, and update it as necessary.
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall	Removed "examples, " to eliminate	Proposed CIP-002-4 Requirement R2: R2. Critical Cyber Asset Identification — Using the list of Critical Assets

Standard: CIP-002-4		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Requirements in CIP-002-4 (Comments)**
develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a control center; or, R3.3. The Cyber Asset is dial-up accessible.	confusion and interpretation issues. Added a qualification for multiple generators at a single plant location. Renumbered to R2.	developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.2. The Cyber Asset uses a routable protocol within a control center; or, R2.3. The Cyber Asset is dial-up accessible.
R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-	Removed reference to R3. Renumbered to R3.	Proposed CIP-002-4 Requirement R3: R3. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if

Standard: CIP-002-4		
Requirement in Approved Standard	**Translation to New Standard or Other Action**	**Requirements in CIP-002-4 (Comments)**
based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)		such lists are null.)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the link below to submit comments on the proposed CIP-002-4. Comments must be submitted by **November 3, 2010.** If you have questions please contact Howard Gugel at howard.gugel@nerc.net or by telephone at (609) 651-2269.

https://www.nerc.net/nercsurvey/Survey.aspx?s=67666bc38c31423dab1ccabfc6f49056

Background:
In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order 706. Version 2 of the standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order 706 directives. Most recently, CIP-010 and CIP-011were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT limited the scope of requirements in this posting of CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in FERC Order 706, paragraph 236. The approach to address the remaining FERC Order 706 directives continues to be developed.

The SDT believes the NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets

associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the "bright-line" criteria contained in *Attachment 1 – Critical Asset Criteria* of the draft CIP-002-4 standard.

The draft CIP-002-4 standard and requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of

deliberation and industry input, the SDT is continuing to evolve the Reliability Standards addressing cyber security by presenting a draft standard *CIP 002-4 – Cyber Security – Critical Cyber Asset Identification* that identifies BES Cyber Systems according to "bright-line" criteria associated with the impact on reliable operation of the BES. The *CIP-002-4 Cyber Security - Critical Asset Identification - Rationale and Implementation Reference Document* provides clarifying notes and rationale of the SDT. The draft CIP-003-4 through CIP-009-4 standards include a set of minimal conforming changes to match the versioning of CIP-002-4.

The bright line criteria included as "Attachment 1" in CIP-002-4 was developed by condensing the list facilities, systems, and other assets that affect BES operations originally developed for CIP-010.

A separate ballot is being conducted for the proposed changes to CIP-005-4 that are being addressed as Urgent Action modifications under Project 2010-15. If the proposed changes to CIP-005-4 are approved under the Urgent Action process, the standard will be modified so that all references within the standard to other CIP standards will reference the correct "Version 4" CIP standard. If the proposed CIP-005-4 is rejected, then CIP-005-3 will be modified with conforming changes (to correctly reference Version 4 CIP standards) and filed with CIP-002-4 to CIP-009-4.

The team is continuing to work on subsequent cyber security standards that will establish impact levels and define associated cyber security controls at levels appropriate to their BES impact.

The team is seeking confirmation that the bright line criteria included in CIP 002-4 is correct and captures all of the facilities, systems, and assets that are essential to the BES. Industry feedback will be considered by the SDT in making additional refinements to CIP 002-4 and its associated documents.

The SDT has provided a form for industry participants to offer their comments on this draft of CIP-002-4, the implementation plans, and the guidance document.

Questions

Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace?

   ☐ Yes

   ☐ No

   Comments:

2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

   ☐ Disagree

   Comments:

4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Agree

☐ Disagree

Comments:

5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it was used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan.[2]

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the Critical Asset identification. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets.'

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009, in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category,' which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program,[3] independent of the determination of a newly identified Critical Cyber Asset.

In all cases where a *Compliant* milestone is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone listed in this Implementation Plan.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [See (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation. (Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in

corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

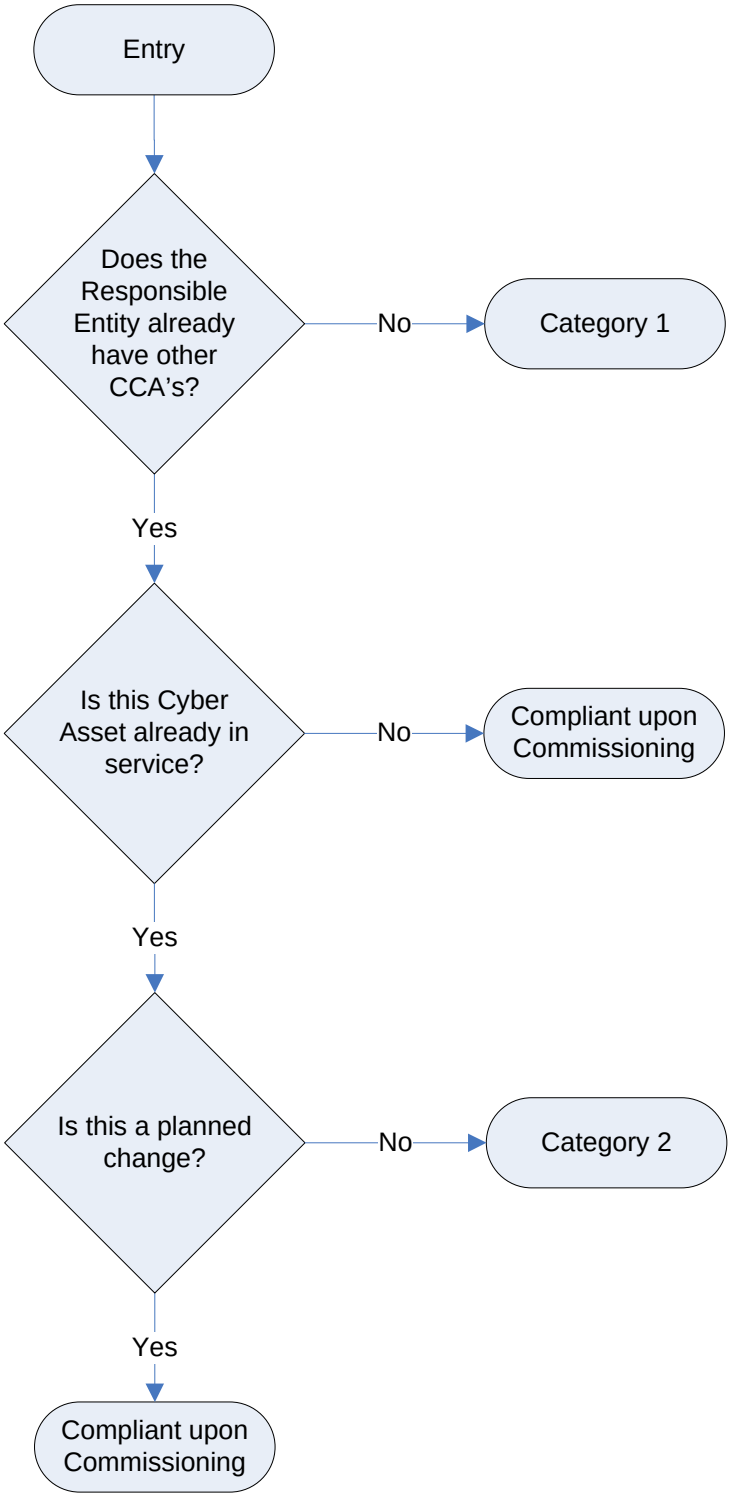


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate Critical Asset identification processes while determining how to either combine the Critical Asset identification processes, or at a minimum, operate separate Critical Asset identifications under a common Senior Manager and governance structure. It would be preferred that a single program be the result, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of the Critical Asset identification as required in CIP-002 R1, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate processes, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform

annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing Critical Asset identification process and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the Critical Asset identification. This scenario will be discussed in two sections, the first dealing with the combination of the Critical Asset identification processes; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the Critical Asset identification processes: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate Critical Asset identification processes while

determining how to either combine the Critical Asset identification processes, or at a minimum, operate the separate Critical Asset identification processes under a common Senior Manager and governance structure. It would be preferred that a single program be the result, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate Critical Asset identification processes to ensure that, absent extraordinary circumstances, the resulting process produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entities' Critical Asset identification processes, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined Critical Asset identification and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R1 and R2. If additional Critical Assets are identified as a result of the application of the merged Critical Asset identification, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the bulk power system. This 'merge plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering Beyond the Effective Date of CIP-002-4		
	Registration + 12 months	Registration + 24 months
	All Facilities	All Facilities
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4~~2~~ through CIP-009-4~~2 and CIP-002-3 through CIP-009-3~~.

The term "Compliant" in this Implementation Plan is used in the same way that it wa~~i~~s used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required '~~"'~~data,'~~"~~ '~~"~~documents,'~~"~~ '~~"~~documentation,'~~"~~ '~~"~~logs,'~~"~~ and '~~"~~records.'~~"~~".

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of ~~either Version 2 or~~ Version 4~~3~~ of the NERC Reliability Standards CIP-003 through CIP-009[1] ~~on Cyber Security~~ for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the ~~risk-based~~ Critical Asset identification ~~methodology~~. Upon a subsequent annual application of the ~~risk-based~~ Critical Asset identification ~~method~~ in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, ~~and~~ Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2', ~~or~~ '-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009, in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

In all cases where a *Compliant* milestone is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone listed in this Implementation Plan.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC ~~in April 2008~~as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. ~~The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.~~

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the Responsibility Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsibility Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria ~~or thresholds~~ in the CIP-002-4 *Attachment 1 Critical Asset Criteria* ~~Responsible Entity's existing risk-based~~ through the application of the Critical Asset identification ~~method~~ (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of ~~that risk-based~~ those Critical Asset criteria ~~Critical Asset Identification process~~ is required annually (by CIP-002 R1~~2~~), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

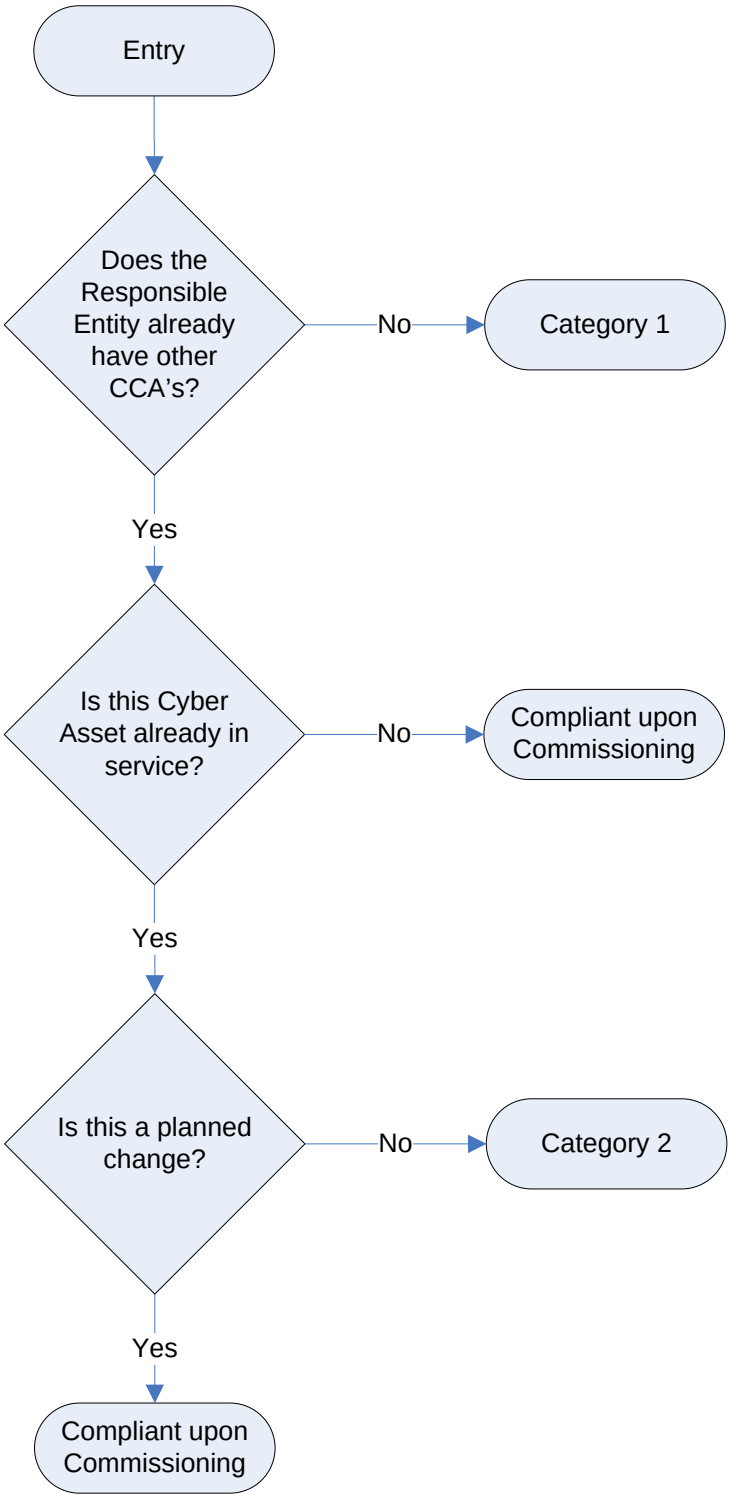


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on ~~planning or impact studies~~the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4~~, and have existing risk-based Critical Asset identification methodologies~~implementations~~~~.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per ~~the~~ NERC Reliability Standard CIP-002-4~~ risk-based Critical Asset identification methodology implementation by each predecessor Responsible Entity~~.

   The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate ~~risk-based~~ Critical Asset identification ~~methodology implementation~~processes while determining how to either combine the ~~risk-based~~ Critical Asset identification~~ methodologies~~s processes~~8ethodologies~~, or at a minimum, operate separate ~~risk-based~~ Critical Asset identifications ~~methodologies~~ under a common Senior Manager and governance structure. It would be preferred that a single program be the result~~ of this analysis~~, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

   The merged Registered Entity must ensure that it maintains the required 'annual application' of ~~risk-based~~the Critical Asset identification ~~methodology(ies)~~ as required in CIP-002 R1~~2~~, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate ~~methodologies~~processes, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the

program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.

If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the ~~risk-based~~ Critical Asset identification ~~methodology~~ as required in CIP-002 R1~~2~~, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 ~~R3~~R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 ~~risk-based~~ Critical Asset identification ~~methodology~~ process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one existing ~~risk-based~~ Critical Asset identification ~~methodology~~ process and more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as -‘simple’ as selection of different anti-virus tools, to something as- ‘~~‘~~complicated’ as ~~risk-based~~the Critical Asset identification ~~methodology~~. This scenario will be discussed in two sections, the first dealing with the combination of ~~risk-based~~the Critical Asset identification

~~methodologies~~processes; the second dealing with combining the CIP compliance implementation programs.

(a) Combining the ~~risk-based~~ Critical Asset identification ~~methodologies~~processes: The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate ~~risk-based~~ Critical Asset identification ~~methodologies~~ processes while determining how to either combine the ~~risk-based~~ Critical Asset identification processes ~~methodologies~~, or at a minimum, operate the separate ~~risk-based~~ Critical Asset identification processes ~~methodologies~~ under a common Senior Manager and governance structure. It would be preferred that a single program be the result ~~of this analysis~~, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.

Registered Entities are encouraged when combining separate ~~risk-based~~ Critical Asset identification ~~methodologies~~ processes to ensure that, absent extraordinary circumstances, the resulting ~~methodology~~ process produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered ~~Entity's~~Entities' ~~risk-based~~ Critical Asset identification ~~methodologies~~processes, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined ~~risk-based~~ Critical Asset identification ~~methodology~~ and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R1~~2~~ and R2~~3~~. If additional Critical Assets are identified as a result of the application of the merged ~~risk-based~~ Critical Asset identification ~~methodology~~, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.

(b) Combining the CIP compliance implementation programs: The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset.

Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the ~~B~~bulk power ~~S~~system. This -'merge plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merge plan is being performed. Progress towards meeting milestones and completing the merge plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly designated Critical Asset, but no newly designated Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4~~2~~ — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
~~R4~~	~~*N/A*~~	~~*N/A*~~
Standard CIP-003-4~~2~~ — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4~~2~~ — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4~~2~~ — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4~~2~~ — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
R8	24 months	12 months
Standard CIP-007-4~~2~~ — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4~~2~~ — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4~~2~~ — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5] Compliance Schedule for Standards CIP-002-42 through CIP-009-42 or CIP-002-3 through CIP-009-3 For Entities Registering in April 2008 and Thereafter Beyond the Effective Date of CIP-002-4		
	Registration + 12 months	Registration + 24 months
	All Facilities	All Facilities
Standard CIP-002-2 or CIP-002-43 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-2 or CIP-003-43 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-2 or CIP-004-43 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-2 or CIP-005-43 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-2 or CIP-006-43 — Physical Security		
All Requirements		Compliant
Standard CIP-007-2 or CIP-007-43 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-2 or CIP-008-43 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-2 or CIP-009-43 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before these standards can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s) [1]
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4

Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard.

[1] CIP-005-4 is being processed as an Urgent Action revision under Project 2010-15 and includes modifications to one of the requirements. CIP-005-4 will be modified and added to the set of standards in this implementation plan so that it has correct references to associated "Version 4" CIP standards after it has completed its balloting through the Urgent Action process.

Proposed Effective Date for CIP-003-4 – CIP-009-4

Critical Cyber Assets Already in Compliance with CIP-003-3 – CIP-009-3
Critical Cyber Assets identified by CIP-002-4 R2 that are already compliant with CIP-003-3 through CIP-009-3 shall be compliant with the requirements of CIP-003-4 through CIP-009-4 on the Effective Date specified in each Version 4 Standard.

Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4
U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 by the latter of (i) 18 months after the Effective Date of CIP-002-4 or (ii) 6 months following the completion of the first refueling outage beyond 18 months from the Effective Date of CIP-002-4 for those requirements requiring a refueling outage.

All Facilities Other Than U.S. Nuclear Power Plant Facilities
For Responsible Entities who previously identified Critical Cyber Assets under CIP-002-1 R3, CIP-002-2 R3, or CIP-002-3 R3; Critical Cyber Assets associated with Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4.

All Other Critical Cyber Assets
For all cases not identified above, Critical Cyber Assets shall be compliant with the requirements of **CIP-003-4 through CIP-009-4** by the latter of (i) the Effective Date specified in each Version 4 Standard or (ii) the compliance milestones in the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* based on the earliest date of identification of the Critical Cyber Asset from CIP-002-1 R3, CIP-002-2 R3, CIP-002-3 R3, or CIP-002-4 R2.

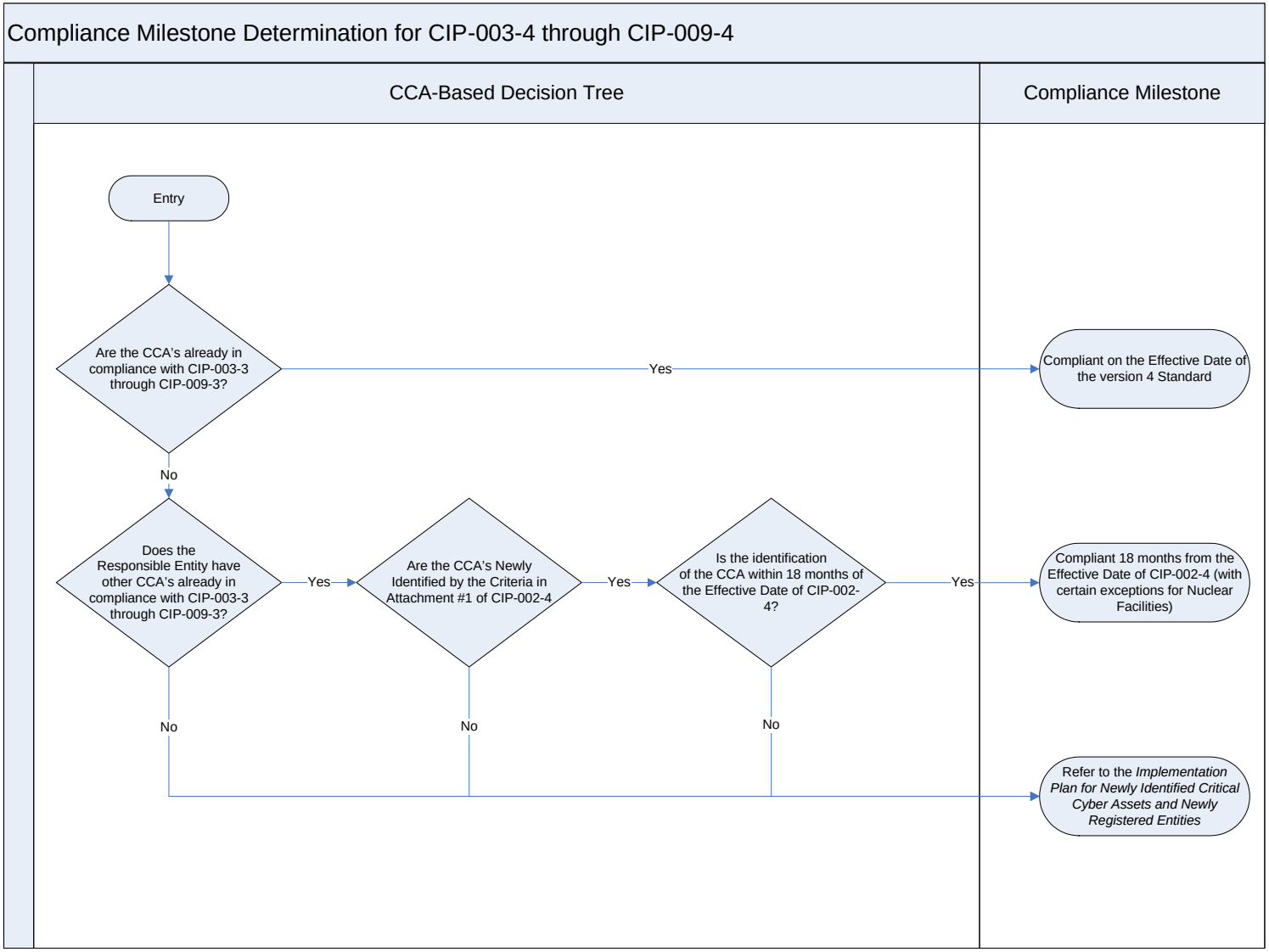
Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document for use by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation Plan will apply based on the situations identified in the above section, *Proposed Effective Date*. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Prior Version Standard Retirements

Standards CIP-002-3 – CIP-009-3 shall be retired upon the Effective Date of the corresponding Version 4 Standards.


Compliance Milestone Determination for CIP-003-4 through CIP-009-4
CCA-Based Decision Tree
Compliance Milestone
Entry
Are the CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Compliant on the Effective Date of the version 4 Standard
No
Does the Responsible Entity have other CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Are the CCA's Newly Identified by the Criteria in Attachment #1 of CIP-002-4
Yes
Is the identification of the CCA within 18 months of the Effective Date of CIP-002-4?
Yes
Compliant 18 months from the Effective Date of CIP-002-4 (with certain exceptions for Nuclear Facilities)
No
No
No
Refer to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.2 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all

reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update

A. Introduction

On October 20, 2010 the following correction was made:

On Page 1 the Applicability Section was corrected to remove what had been 4.2.1:

> Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~3~~4

3. **Purpose:** Standard CIP-008-~~3~~ 4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-~~23~~ 4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~ 4 through CIP-009-~~3~~4.

4. **Applicability**

   4.1. Within the text of Standard CIP-008-~~3~~4, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-008-~~3~~4:

   ~~**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.~~

   ~~4.2.2~~4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   ~~4.2.3~~4.2.2 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-~~3~~ 4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R2.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R2.2. The Cyber Asset uses a routable protocol within a control center; or,

R2.3. The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.

1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes.

1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.

1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.

1.16. Any additional assets that the Responsible Entity deems appropriate to include.

A. Introduction

On October 20, 2010 the following correction was made:

R3 on Page 4 was corrected to remove the following phrase:

. . . the risk based assessment methodology, . . .

1. **Title:** Cyber Security — Critical Cyber Asset Identification

2. **Number:** CIP-002-~~3~~4

3. **Purpose:** NERC Standards CIP-002-~~3~~ 4 through CIP-009-~~3~~ 4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-~~3~~ 4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1~~a risk-based assessment~~.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-~~3~~4, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-002-~~3~~4:

   ~~**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.~~

   ~~**4.2.2**~~**4.2.1** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~**R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.~~

~~**R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.~~

~~**R1.2.** The risk-based assessment shall consider the following assets:~~

~~**R1.2.1.** Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.~~

~~**R1.2.2.** Transmission substations that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.3.** Generation resources that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.4.** Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.~~

~~**R1.2.5.** Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.~~

~~**R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.7.** Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.~~

~~**R2.**~~**R1.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*~~risk-based assessment methodology required in R1~~. The Responsible Entity shall review this list at least annually, and update it as necessary.

~~**R3.**~~**R2.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1~~2~~, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes.~~Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange.~~ The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-~~3~~4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

~~**R3.1.**~~**R2.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

~~**R3.2.**~~**R2.2.** The Cyber Asset uses a routable protocol within a control center; or,

~~**R3.3.**~~**R2.3.** The Cyber Asset is dial-up accessible.

~~**R4.**~~**R3.** Annual Approval — The senior manager or delegate(s) shall approve annually ~~the risk-based assessment methodology,~~ the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1~~, R2,~~ and R2~~3~~ the Responsible Entity may determine that it has no

Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

~~**M1.** The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.~~

~~**M2.**~~**M1.** The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1~~2~~.

~~**M3.**~~**M2.** The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2~~3~~.

~~**M4.**~~**M3.** The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3~~4~~.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~3~~ 4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.

1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes.

1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.

1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.

1.16. Any additional assets that the Responsible Entity deems appropriate to include.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Ballot Pool Formation September 20-October 20, 2010
Formal Comment Period September 20-November 3, 2010
Project 2008-06 — Cyber Security 706

Now available at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Project 2008-06 — Cyber Security 706

A set of proposed changes to CIP-002-3 - Cyber Security — Critical Cyber Asset Identification, associated implementation plans, and conforming changes to several other CIP standards have been posted for stakeholder review. These are considered, "Version 4 CIP Standards." The drafting team also developed and posted a mapping document to show the translation of requirements from CIP-002-3 to CIP-002-4, and a guidance document to assist in applying the proposed CIP-002-4 standard.

The proposed CIP-002-4 provides a significant improvement to CIP-002-3 by including a specific list of criteria for entities to use in identifying their critical assets.

The previously approved versions of CIP-002 relied on entities to develop their own critical asset identification methodology, and have led to unequal assessments of critical assets between entities in a region, and between regions. This subjectivity has led some external observers to question how assessments were produced, and has contributed to distrust of the entire critical asset identification process. The revised standard provides uniformity to the critical asset identification process for all entities as well as uniformity and predictability to the audit process. As envisioned, each entity will apply the criteria against its assets to determine exactly which side of the "bright-line" they fall. The bright-line thresholds are justified based on overall impact to Bulk Electric System reliability, adding further clarity to the critical asset identification process. The bright-line criteria were developed based on stakeholder comments on CIP-010.

Recognizing that protecting the cyber assets critical to the electric utility's infrastructure is also critical to national and international security, the revisions to CIP-002 are being advanced ahead of other improvements to the remaining set of CIP standards. The remaining CIP standards all rely on a complete and accurate identification of those assets that are critical to reliability. Because entities are so tightly interconnected, a vulnerability that seems insignificant to a single entity can place the entire grid in a state of vulnerability.

Each of the CIP standards (CIP-003-3 through CIP-009-3) contains at least one reference to CIP-002-3. To maintain clarity, CIP-003-3 through CIP-009-3, have had conforming changes made so that all cross references within the set of standards are to "CIP Version 4" standards. *(CIP-005-4 - Cyber Security — Electronic Security Perimeter is posted separately, with a set of proposed revisions for Urgent Action under Project 2010-15. If CIP-005-4 is not approved as an Urgent Action, it will be returned to this set of CIP standards.)*

Ballot Pool Open through Morning of October 20, 2010

Registered Ballot Body members may join the ballot pool **until 8 a.m. Eastern on October 20, 2010** to be eligible to vote in the upcoming ballot for the CIP Version 4 standards at the following page:

https://standards.nerc.net/BallotPool.aspx

Until the ballot begins, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list server.) The list server for this ballot pool is: bp-2008-06_CIPv4_in@nerc.com

Formal 45-day Comment Period Open through November 3, 2010

Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Transition from Reliability Standards Development Procedure Version 7 to Standard Processes Manual

Under the Reliability Standards Development Procedure Version 7, consensus was built with successive formal comment periods, followed by a 30-day pre-ballot review, followed by an initial ballot, and then a recirculation ballot. The intent was to use stakeholder views submitted through the formal comment periods to achieve consensus, and then to confirm that consensus during the balloting. This process did not allow a drafting team to make any changes to a standard between ballots, which incented teams to avoid making improvements once a standard had gone through an initial ballot. If a team made a change between ballots, then the standard was required to be posted for a new comment period and then another pre-ballot review and another initial ballot. Finally if there were no more changes made to the standard, a recirculation ballot was conducted to confirm consensus.

Under the new Standard Processes Manual, consensus is achieved through parallel comment and ballot periods. Successive comment and ballot periods are conducted until there is consensus – and then a recirculation ballot is conducted to confirm that consensus. There is no 30-day pre-ballot review period, and drafting teams are encouraged to make revisions to the standard between successive ballots to improve the quality of the standard.

Next Steps

During the last 10 days of the 45-day formal comment period, an initial ballot will be conducted. (The drafting team is not proposing any modifications to existing Violation Risk Factors (VRFs) or Violation Severity Levels (VSLs); thus, there will not be a poll to assess stakeholder views of the VRFs and VSLs.) The drafting team will consider all stakeholder comments (those submitted with a comment form, and those submitted with a ballot) and will determine whether to make additional changes to the standards and implementation plans. The team will post its response to comments and, if the team has made only minor changes, the team will post the standards and implementation plan and conduct a 10-day recirculation ballot.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

For more information or assistance, please contact Monica Benson,
Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Consideration of Comments on Cyber Security Order 706 Phase II — Draft CIP-002-4 Project 2008-06

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the proposed CIP-002-4. These standards were posted for a 45-day public comment period from September 20, 2010 through November 3, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 101 sets of comments, including comments from more than 200 different people from approximately 125 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

Based on the comments received, a few changes were made to CIP-002-4. The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. In addition, the effective date was changes to eight quarters after regulatory approval, so that entities are not required to maintain two sets of approved Critical Asset lists and Critical Cyber Asset lists during the implementation plan. Requirements R1 and R2 were modified slightly to clarify that each list must be updated on an ongoing basis, but the review and approval need only occur annually. Conforming changes were made to the compliance section. Finally, changes were made to Attachment 1. A brief summary of each change can be found in the summary response to question 2 on page 33.

The modified CIP-002-4 will be posted for a ten day concurrent ballot and comment period. The SDT will review the comments and determine any necessary changes to CIP-002-4 based on the ballot. In addition, NERC staff will conduct a webinar on the changes during the comment and ballot period.

A complete record of this project, including clean and redline versions of the revised standard that commenters reviewed, is posted on the project page on the NERC website at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace? 15

2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement..... 35

3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.. 166

4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 179

5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement..... 199

6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement. . 223

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Gregory Campoli	New York Independent System Operator	NPCC	2
3.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Michael Schiavone	National Grid	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Dean Ellis	Dynegy Generation	NPCC	5
8.	Saurabh Saksena	National Grid	NPCC	1
9.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5
11.	Kathleen Goodman	ISO - New England	NPCC	2
12.	Chantel Haswell	FPL Group, Inc.	NPCC	5
13.	David Kiguel	Hydro One Networks Inc.	NPCC	1
14.	Michael R. Lombardi	Northeast Utilities	NPCC	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Randy MacDonald	New Brunswick System Operator	NPCC 2										
16.	Bruce Metruck	New York Power Authority	NPCC 6										
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC 10										
18.	Robert Pellegrini	The United Illuminating Company	NPCC 1										
2.	Group	David Grubbs	City of Garland	X									

	Additional Member	Additional Organization	Region	Segment Selection
1.	Fred Sherman		ERCOT	1
2.	Billy Lee		ERCOT	1
3.	Ronnie Hoeinghaus		ERCOT	1
4.	William Whitney		ERCOT	1
5.	Heather Siemens		ERCOT	1

3.	Group	Patricia Lynch	NRG Energy Inc.					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Energy Power Marketing Inc	NA - Not Applicable	3
2.	Richard Comeaux	Louisiana Generating LLC	SERC	4
3.	Alan Johnson	NRG Energy Inc.	NA - Not Applicable	6

4.	Group	Nathan Mitchell	APPA CIP-002-4 Task Force	X		X	X	X			X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Allen Mosher	APPA	NA - Not Applicable	4
2.	Nathan Mitchell	APPA	NA - Not Applicable	3
3.	Doug Bantam	LES	MRO	1
4.	Bruce Merrill	LES	MRO	3
5.	Dennis Florom	LES	MRO	5
6.	Eric Ruskamp	LES	MRO	6
7.	Brian Evens-Mongeon	Utility Services	NA - Not Applicable	8
8.	Steve Alexanderson	Central Lincoln	WECC	3, 4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
9.	Mike Stanley	MEAG	SERC 1										
10.	Danny Dees	MEAG	SERC 3										
11.	Scott Miller	MEAG	SERC 5										
5.	Group	Ben Li	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patrick Brown	PJM	RFC	2
2.	Matthew Goldberg	ISO NE	NPCC	2
3.	Greg Campoli	NY ISO	NPCC	2
4.	Mark Thompson	AESO	WECC	2
5.	Charles Yeung	SPP	SPP	2
6.	Steve Myers	ERCOT	ERCOT	2
7.	Greg Van Pelt	CA ISO	WECC	2
8.	Bill Phillips	MISO	RFC	2
9.	Matt Morias	ERCOT	ERCOT	2
10.	Kathleen Goodman	ISO NE	NPCC	2
11.	Jason Marshall	MISO	RFC	2
12.	Albert DiCaprio	PJM	RFC	2

6.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.		Dick Winters	BPA, Transmission, Substation Operations	WECC 1
2.		Curt Wilkins	BPA, Transmission, Control Cntr HW Design & Maint	WECC 1

7.	Group	Kenneth D. Brown	PSEG Companies	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.		Jeff Mueller	PSE&G	RFC 1, 3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2.		Jerzy Slusarz	PSEG Fossil RFC 5, 6										
3.		Jim Hebson	PSEG ER&T NPCC 5, 6										
4.		Dom Grasso	Odessa Ector LP ERCOT 5, 6										
8.	Group	Richard J. Kafka	Pepco Holdings, Inc - Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Godfrey	Delmarva Power & Light	RFC	1
2.	Mark Yerger	Delmarva Power & Light	RFC	1
3.	Dave Throne	Potomac Electric Power Company	RFC	1

9.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										X

Additional Member	Additional Organization	Region	Segment Selection
1.	Mahmood Safi	Omaha Public Utility District	MRO	1, 3, 5, 6
2.	Chuck Lawrence	American Transmission Company	MRO	1
3.	Tom Webb	WPS Corporation	MRO	3, 4, 5, 6
4.	Jason Marshall	Midwest ISO Inc.	MRO	2
5.	Jodi Jenson	Western Area Power Administration	MRO	1, 6
6.	Ken Goldsmith	Alliant Energy	MRO	4
7.	Alice Murdock	Xcel Energy	MRO	1, 3, 5, 6
8.	Dave Rudolph	Basin Electric Power Cooperative	MRO	1, 3, 5, 6
9.	Eric Ruskamp	Lincoln Electric System	MRO	1, 3, 5, 6
10.	Joseph Knight	Great River Energy	MRO	1, 3, 5, 6
11.	Joe DePoorter	Madison Gas & Electric	MRO	3, 4, 5, 6
12.	Scott Nickels	Rochester Public Utilties	MRO	4
13.	Terry Harbour	MidAmerican Energy Company	MRO	1, 3, 5, 6

10.	Group	Terry L. Blackwell	Santee Cooper	X		X		X	X				

Additional Member	Additional Organization	Region	Segment Selection

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10
1. S. Tom Abrams	Santee Cooper	SERC 1, 3, 5, 6										
2. Rene' Free	Santee Cooper	SERC 1, 3, 5, 6										
3. Glenn Stephens	Santee Cooper	SERC 1, 3, 5, 6										
4. Jim Peterson	Santee Cooper	SERC 1, 3, 5, 6										
5. Wayne Ahl	Santee Cooper	SERC 1, 3, 5, 6										
6. Vicky Budreau	Santee Cooper	SERC 1, 3, 5, 6										
11. Group	Louis Slade	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Garton	Electric Market Policy	MRO	5, 6
2.	Carl Eng	Electric Transmission	SERC	1, 3
3.	Jeff Heffleman	F&H generation	SERC	5
4.	Jeff Bailey	Nuclear		5
5.	Bruce Bingham	IT Risk Mgt.		NA
6.	John Calder	Electric Transmission Compliance	SERC	1, 3
7.	Marc Gaudette	IT Risk Mgt.		NA
8.	John Mitchell	ELECTRIC TRANSMISSION	SERC	1, 3
9.	Don Robinson	IT GENERATION		NA

12. Group	John P. Falsey	Edison Mission Marketing and Trading					X					

Additional Member	Additional Organization	Region	Segment Selection
1.	Ellen L. Oswald	NA - Not Applicable	5
2.	Brenda J. Frazer	RFC	5
3.	James W. Thompson	WECC	5

13. Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	Utilities Commission, City of New Smyrna Beach	FRCC	4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2. Greg Woessner		Kissimmee Utility Authority	FRCC 3										
3. Jim Howard		Lakeland Electric	FRCC 3										
4. Lynne Mila		City of Clewiston	FRCC 3										
5. Joe Stonecipher		Beaches Energy Services	FRCC 1										
6. Cairo Vanegas		Fort Pierce Utility Authority	FRCC 4										
7. Randy Hahn		Ocala Electric Utility	FRCC 3										
14.	Group	Ron Sporseen	PNGC Power	X		X					X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bud Tracy	Blachly-Lane Electric Cooperative	WECC	3, 8
2.	Dave Markham	Central Electric Cooperative	WECC	3, 8
3.	Dave Hagen	Clearwater	WECC	3, 8
4.	Roman Gillen	Consumer's Power	WECC	1, 3, 8
5.	Roger Meader	Coos-Curry Electric Cooperative		3, 8
6.	Dave Sabala	Douglas Electric Cooperative		8
7.	Bryan Case	Fall River Electric Cooperative		3, 8
8.	Rick Crinklaw	Lane Electric Cooperative		3, 8
9.	Michael Henry	Lincoln Electric Cooperative		8
10.	Richard Reynolds	Lost River		8
11.	Jon Shelby	Northern Lights		3, 8
12.	Ray Ellis	Okanogan		8
13.	Heber Carpenter	Raft River		3, 8
14.	Ken Dizes	Salmon River Electric Coop		1, 3, 8
15.	Steve Eldrige	Umatilla Electric Coop		1, 3, 8
16.	Marc Farmer	West Oregon Electric Coop		8

15.	Individual	Steve Rueckert	WECC										X
16.	Individual	JT Wood	Southern Company	X		X							

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
17.	Individual	Steven Hamburg	Encari, LLC								X		
18.	Individual	Janet Smith	Arizona Public Service	X		X		X	X				
19.	Individual	David Batz	Edison Electric Institute										
20.	Individual	James W. Sample	Tennessee Valley Authority (TVA)	X		X		X	X				
21.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
22.	Individual	Larry Saxon	OGE	X		X		X					
23.	Individual	J. Randall McCamish	FMPA	X		X							
24.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
25.	Individual	Kelsi Oswald	Pinellas County Resource Recovery Facility					X					
26.	Individual	Steve Alexanderson	Central Lincoln			X							
27.	Individual	John Falsey	Edison Mission Marketing and Trading					X					
28.	Individual	James Stanton	SPS Consulting Group Inc.								X		
29.	Individual	Scott Amsden	Tacoma Power	X		X	X	X	X				
30.	Individual	Greg Froehling	Green Country Energy					X					
31.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
32.	Individual	Richard Burt	Minnkota Power Cooperative	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	J. Brent Hebert	Horizon Wind Energy					X					
34.	Individual	Larry Rodriguez	Union Power Partners LP						X				
35.	Individual	Todd Williams	MidAmerican Energy Company	X		X		X	X				
36.	Individual	Gary Ofner	North Carolina Membership Corporation	X		X	X	X					
37.	Individual	Sasa Maljukan	Hydro One Networks Inc.	X									
38.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
39.	Individual	Donovan Tindill	Matrikon Inc.	N/A									
40.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
41.	Individual	John Brockhan	CenterPoint Energy	X		X							
42.	Individual	Edward Nagy	LCEC	X		X							
43.	Individual	Jon Kapitz	Xcel Energy	X		X		X	X				
44.	Individual	Joe Knight	Great River Energy	X		X		X	X				
45.	Individual	Michael Moltane	ITC Holdings	X									
46.	Individual	Jack Stamper	Public Utility District No. 1 of Clark County	X									
47.	Individual	Jian Zhang	TransAlta	X				X	X				
48.	Individual	John Bee	Exelon	X		X		X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
49.	Individual	John Bussman	AECI	X		X		X	X				
50.	Individual	Mark Ramsey	N.W. Electric Power Cooperative, Inc.	X		X							
51.	Individual	Michael Bax	Central Electric Power Cooperative	X		X							
52.	Individual	Ralph Schulte	Central Electric Power Cooperative	X		X							
53.	Individual	Stephen Pogue	M & A Electric Power Cooperative			X							
54.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
55.	Individual	Denise Stevens	Sho-Me Power Electric Cooperative	X									
56.	Individual	Ted Hilmes	KAMO Power			X							
57.	Individual	Jonathan Appelbaum	United Illumiinating	X									
58.	Individual	Brenda Powell	Constellation Energy Commodities Group						X				
59.	Individual	Brian Ackermann	Associated Electric Cooperative, Inc.						X				
60.	Individual	Walter Kenyon	KAMO Electric Cooperative	X		X							
61.	Individual	Kevin White	Northeast Missouri Electric Power Cooperative	X									
62.	Individual	David McDowell	NW Electric Power Cooperative, Inc.	X		X							
63.	Individual	Rich Salgo	Sierra Pacific Power d/b/a NV Energy	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
64.	Individual	Jeff Neas	Sho-Me Power Electric Cooperative			X							
65.	Individual	Matt Brewer	SDG&E	X		X		X					
66.	Individual	Steve Alexanderson	Central Lincoln			X	X						
67.	Individual	Skyler Wiegmann	Northeast Missouri Electric Power Cooperative			X							
68.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
69.	Individual	Art Baum	Tampa Electric	X		X		X					
70.	Individual	William Price	M&A Electric Power Cooperative	X									
71.	Individual	Scott Miller	MEAG Power	X		X		X					
72.	Individual	Chris Bolick	Associated Electric Cooperative, Inc.	X		X		X	X				
73.	Individual	Brad Haralson	Associated Electric Cooperative, Inc.	X		X		X	X				
74.	Individual	Doug Hohlbaugh	FirstEnergy Corp	X		X	X	X	X				
75.	Individual	Randi Woodward	Minnesota Power	X		X		X	X				
76.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
77.	Individual	Andrew Z. Pusztai	American Transmission Company	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
78.	Individual	Kirit Shah	Ameren	X		X		X	X				
79.	Individual	Bill Keagle	BGE	X									
80.	Individual	J. S. Stonecipher, PE	Beaches Energy Services (of City of Jacksonville Beach, FL)	X								X	
81.	Individual	Jim Keller	We Energies			X	X	X					
82.	Individual	John Allen	City Utilities of Springfield, MO	X									
83.	Individual	Saurabh Saksena	National Grid	X		X							
84.	Individual	Eric Ruskamp	Lincoln Electric System	X		X		X	X				
85.	Individual	Kevin B. Perry	Southwest Power Pool Regional Entity		X								X
86.	Individual	Jerry Hohn	Indianapolis Power & Light	X									
87.	Individual	Amir Hammad	Constellation Power Generation					X					
88.	Individual	Dan Rochester	Independent Electricity System Operator		X								
89.	Individual	Thad Ness	American Electric Power (AEP)	X		X		X	X				
90.	Individual	Richard Kinas	Orlando Utilities Commission	X		X		X	X				
91.	Individual	Scott McGough	Oglethorpe Power Corporation						X				
92.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X		X		X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
93.	Individual	Jason Marshall	Midwest ISO		X								
94.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
95.	Individual	Steven Wallace	Seminole Electric Cooperative, Inc.			X	X	X	X				
96.	Individual	Peter Brown	Progress Energy	X		X		X	X				
97.	Individual	Brad Chase	Orlando Utilities Commission	X		X		X	X				
98.	Individual	Gregory Campoli	New York Independent System Operator		X								
99.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
100.	Individual	Richard Kinas	Orlando Utilities Commission	X		X		X	X				
101.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X				

1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace?

Summary Consideration: Many of those that voted "No" contended their current risk-based methodology provided a more accurate list of Critical Assets and therefore the proposed criteria in Attachment 1 would not lead to an improvement in reliability. Often, those who commented this way also felt the criteria did not have rigorous system studies as a reliability basis.

The SDT appreciates these comments but believes that although some companies may have a very rigorous risk-based assessment, the implementation of Attachment 1 criteria will overall increase the consistency of Critical Asset identification. The Attachment 1 criteria were developed in response to an external oversight directive in the FERC Order 706. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. The "bright-line" criteria approach removes the variability of entity-defined methodologies that would prompt the need for external review.

Regarding the need for additional engineering studies, the SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. The industry provided significant feedback for the need to simplify the Critical Asset identification approach. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. NERC issued a data request in August of 2010 to assist the SDT in developing a consistent approach to Critical Asset identification. The results of this request were used to assist the team in developing the criteria in Attachment 1.

A few commenters expressed concern that changes to these Standards do not address other significant issues. The SDT agrees that other changes ultimately need to be made to the body of CIP cyber security standards, and expects to resume working on those in early 2011. The scope of the changes to the interim CIP-002-4 was deliberately limited to minimize the impact on the industry while addressing the identified consistency issues with the Critical Asset identification method.

Organization	Yes or No	Question 1 Comment
Northeast Power Coordinating Council	No	The proposed Standard improves implementation consistency which may improve reliability, and it will lead to an improvement in reliability for entities that are either newly registered, or envision new assets coming under their CIP purview. Improved reliability overall however, is not guaranteed. The proposed standard can lead to an improvement in reliability by being entirely prescriptive and allowing for no flexibility for the Responsible Entity in determining critical assets. A risk-based methodology for identifying critical assets is similar to the bright-line criteria proposed in the revision for CIP-002, and it makes an asset list very inclusive. The proposed standard will not lead to a significant improvement in reliability because it will not result in a significant increase in the number of assets identified as critical. Replacing the risk-based assessment methodology with a list of criteria will ultimately result in the inclusion of facilities on the Critical Assets list that are non-impactive to the BES. Per paragraph 236 of FERC Order 706, the proposed standard does provide guidance regarding the risk-based assessment methodology and scope of critical assets. However, the proposed standard does not address guidance on external review of critical assets identification. This may be implied by the prescriptive nature of the assets listed in Attachment 1. External review was specifically called for in the FERC Order.Per paragraph 253, the Commission stresses "the need for flexibility and the need to take account of the individual circumstances of a responsible entity". This is not accomplished under prescriptive approach to the proposed standard. The proposed revision replaces the existing risk-based methodology with the new bright-line criteria. The reference to risk-based methodology in R3 should be deleted.The updated Applicability section (4.2.1) removed the U.S. and Canadian nuclear exclusion to CIP-002-4. Order 706B removed the U.S. nuclear exclusion. The Canadian nuclear (facilities regulated by the Canadian Nuclear Safety Commission) exclusion should remain or those assets may be regulated by two different authorities.
Response: Thank you for your comments. Regarding the directives for external review and guidance in the FERC Order, the SDT believes the criteria in Attachment 1 are in response to FERC Order 706 paragraph 329. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This "bright-line" approach removes the variability of entity defined methodologies that would prompt the need for external review.		
City of Garland	No	No way to confirm that the criteria in attachment 1 will improve reliability over the risk based assessment methodologies developed by Responsible Entities.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
NRG Energy Inc.	No	No we do not believe this will improve reliability significantly. It might provide improvement in what is defined as critical assets.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
APPA CIP-002-4 Task Force	No	APPA Comments: APPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). APPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, APPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW.We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan.
Response: Thank you for your comments. Please refer to the response to your comments on Question 2.		
IRC Standards Review Committee	No	The assets that should be subject to protection under the NERC CIP Standards should not be driven by the physical assets that are implicated in maintaining physical system reliability from an operations and planning perspective. There is not a direct relationship between assets that are subject to protection under the CIP

Organization	Yes or No	Question 1 Comment
		standards and assets that form the basis for the current NERC understanding of planning and operating reliability. Nor should the scope of cyber assets be determined by the identification of physical asset by third parties. Under the current and proposed CIP Standards, the scope of jurisdictional cyber assets is driven by an entity's Critical Assets, which are physical assets that impact system reliability from an operations/planning perspective (i.e. Critical Assets are defined as: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.). In addition, the proposed standards include third party identification of critical assets. The Standards Drafting Team should take this opportunity to eliminate all of these inappropriate relationships. As an initial matter, the SDT should remove the term "Critical Assets" from the standard. This term should be replaced with a general term, such as "Assets Subject to Cyber Security Protection". This change will eliminate the inappropriate cause and effect relationship between physical system reliability - i.e. operations and planning - and cyber security. Instead, the general term directly links the driver of asset identification to cyber security. The next step should focus on the explicit identification of assets that fall within this category. The identification should be based on an objective list of assets. This mitigates the problems that arise from the application of a subjective identification methodology. Attached to these comments is a proposed list, which is intended to be used as a starting point (see proposed Attachment 1 below). The SRC believes this list includes asset types that should be subject to the CIP standards. However, at this point, the list is illustrative and is not intended to be exhaustive. This approach enables the identification of assets that are subject to cyber security protection irrespective of their relationship to the definition of "Critical Asset". By decoupling the assets subject to cyber protection from the subjective "Critical Asset" terminology, the proposed approach actually expands the number of assets that are subject to the CIP standards. This approach is a relative improvement because it provides certainty to the regulated community and the regulators by removing the subjectivity associated with the use of terms such as "critical" or "reliability". In addition to the above recommendations, the SDT should also revise Attachment 1 to explicitly clarify which functional entities are responsible for the relevant asset types. A revised version of Attachment 1 that reflects the above recommendations is provided below. **********CIP-002-4 - Attachment 1 Assets Subject to Cyber Security ProtectionThe following are assets subject to Cyber Security Protection: 1. By the Generation Owner (GO):1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. 1.2. Each resource asset that the GO's Planning Coordinator identifies that if that asset is destroyed, degraded, misused or otherwise rendered unavailable, will violate one or more Interconnection Reliability Operating Limits (IROLs). 1.3. Each Blackstart Resource identified in the GO's Transmission Operator's restoration plan.1.4. Each control center, control system, backup control center, or backup control system used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.1.5. Each GO's Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).2. By the

Organization	Yes or No	Question 1 Comment
		Transmission Owner (TO):2.1. Transmission Facilities operated at 500 kV or higher. 2.2. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.2.3. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.2.4. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. 2.5. Each resource asset that the TO's Planning Coordinator identifies that if that asset is destroyed, degraded, misused or otherwise rendered unavailable, will violate one or more Interconnection Reliability Operating Limits (IROLs). 2.6. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. 2.7. Each TO's Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).2.8. Transmission Facilities identified by a nuclear asset owner as essential to meeting Nuclear Plant Interface Requirements.2.9. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.4. 2.10. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 3. By the Reliability Coordinator3.1. Each control center, control system, backup control center, or backup control system used to perform the RC functional obligations4. By the Transmission Operator4.1. Each control center, control system, backup control center, or backup control system used to perform the TOP functional obligations4.2. Each TOP's Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).5. Balancing Authority5.1. Each control center, control system, backup control center, or backup control system used to perform the BA functional obligations
Response: Thank you for your comments. Please refer to the response to your comments on Question 2.		
Bonneville Power Administration	No	The individual utility's development and implementation of their risk-based methodology instills ownership in their process and is a positive result of the current CIP versions. For BPA, application of the bright-line assessment criteria for Critical Asset identification in the recent NERC data request resulted in fewer assets being classified in the high impact categorization. However, we see that if a utility's implementation of the criteria resulted in more Critical Assets being identified with the corresponding implementation of security controls at those assets, then an improvement in reliability would occur.
Response: Thank you for your comments. While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets		

Organization	Yes or No	Question 1 Comment
in North America will be classified as Critical Assets.		
PSEG Companies	Yes	
Pepco Holdings, Inc - Affiliates	Yes	
MRO's NERC Standards Review Subcommittee	No	If Responsible Entities perform risk based assessments based on Engineering studies, as outlined in the version 3 Identifying Critical Assets reference document, we believe this would provide a more accurate listing of the truly critical assets as opposed to the new bright line approach of version 4. However, if the bright line approach is maintained going forward, we have included suggested improvements to the criteria under question #2.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology. Please refer to the response to comments for Question 2.		
Santee Cooper	No	We have put forth a best faith effort in producing a Vulnerability/Risk Assessment methodology that was thorough and fair. Our methodology produced critical assets that went beyond our control centers. It is our belief that the proposed standard will divert resources from maintaining system reliability to efforts which have little or no benefit. Our concern lies in a new process that will require us to submit large amounts of paperwork for new processes that will hinder rather than enhance system reliability. Many more assets will be arbitrarily added, resulting in large expenditures and personnel time. We would hate for BES reliability to suffer because of a focus shift to certain paperwork for assets which clearly do not impact or marginally impact overall Grid Reliability.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Dominion	Yes	Dominion believes that its Risk Based Methodology is sound in identifying Critical Assets, however we agree the new standard will provide more consistency across the interconnection.
Response: Thank you for your comments.		
Edison Mission Marketing and Trading	No	

Organization	Yes or No	Question 1 Comment
Florida Municipal Power Agency	Yes	However, significant improvements can be made to Attachment 1 as described in the response to Question 2.
Response: Thank you for your comments. Please refer to the response to comments for Question 2.		
PNGC Power	Yes	
WECC		Agree with the approach of a bright line. However, stakeholders have indicated that the current criteria may lead to the identification of fewer Critical Assets. Need to make certain that the bright line criteria is "in the right place" to ensure the appropriate Critical Assets.
Response: Thank you for your comments. While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets in North America will be classified as Critical Assets.		
Southern Company	No	As currently drafted, Southern believes that several of the proposed requirements could lead to a decrease in reliability of the bulk electric system.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Encari, LLC	Yes	
Arizona Public Service	Yes	
Edison Electric Institute	Yes	EEI believes that the adoption of a uniform and consistent methodology for the selection of Critical Assets will enhance the reliability of the bulk power system.
Response: Thank you for your comments.		
Tennessee Valley Authority (TVA)	Yes	None.
PacifiCorp	Yes	PacifiCorp commends the Standards Drafting Team for the current version of proposed CIP-002-4, which is a marked improvement to the standard that is currently effective. The current risk-based assessment methodology allows for inconsistent interpretations of which assets are considered “critical.” Employing the same bright-line Critical Asset criteria for all responsible entities will result in greater consistency and

Organization	Yes or No	Question 1 Comment
		accuracy in the identification of such assets, and thus necessarily an improvement in reliability.
Response: Thank you for your comments.		
OGE	No	These changes benefit in reducing the compliance effort but do not improve reliability of the BES.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
FMPA	Yes	However, significant improvements can be made to Attachment 1 as described in the response to Question 2.
Response: Thank you for your comments. Please refer to the response to comments for Question 2.		
South Carolina Electric and Gas	Yes	
Pinellas County Resource Recovery Facility	No	I don't think that the changes to the standard will decrease or increase reliability, but they do provide much needed clarity to the identification process.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Central Lincoln	Yes	
Edison Mission Marketing and Trading	Yes	
SPS Consulting Group Inc.	No	There is not enough data on historic or potential cyber threats to assess whether the proposed standard will have any affect on reliability.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Tacoma Power	Yes	Tacoma Power commends the SDT for its efforts in revising CIP-002-4. Tacoma Power agrees that the proposed standard will lead to an improvement in reliability when compared to the previous version. The inclusion of Attachment 1 will achieve the result of better defining systems as Critical Assets.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments.		
Green Country Energy	No	However it makes determining critical status much easier on the small generator
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Illinois Municipal Electric Agency	Yes	
Minnkota Power Cooperative	Yes	
Horizon Wind Energy	Yes	
Union Power Partners LP	Yes	Somewhat. However, since the objective from day one has been protecting the BES from malicious manipulation from outside intruders, the wording in R2 should incorporate "Cyber assets accessible from outside the plant" that could - - - .
Response: Thank you for your comments. The set of CIP cyber security standards (CIP-002 to CIP-009) is a holistic approach to cyber security protection that applies to both internal and external threats.		
MidAmerican Energy Company	Yes	CIP-002-4 is a step forward in achieving a uniform and consistent methodology of selecting Critical Assets within the industry.
Response: Thank you for your comments.		
North Carolina Membership Corporation		In the new Requirement R3, there is a reference to the “risk-based assessment methodology.” Under the revised standard there is no longer such a methodology and this language should be removed from the new R3.
Response: Thank you for your comments. Prior to the next ballot, this reference will be removed.		
Hydro One Networks Inc.	No	We do not believe the standard will result in an improvement in reliability since the revisions merely replace the risk-based assessment methodology with a list of criteria that will ultimately result in inclusion of facilities on the Critical Assets list that are non-impactive on the BES. We do not agree with the removal of the exclusion that applies to facilities regulated by the Canadian Nuclear Safety Commission from the

Organization	Yes or No	Question 1 Comment
		Applicability Section, This explicit statement makes it clear that CIP standards do not apply to those facilities which would not be the case if it were removed.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology. The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.		
Dynegy Inc.	No	I think proposed CIP-002-4 can lead to improved reliability but various clarifications need to be made as further discussed below.
Response: Thank you for your comment. Please refer to the response to comments for Question 2.		
Matrikon Inc.	Yes	
Northeast Utilities	Yes	
CenterPoint Energy	No	Whereas CenterPoint Energy does not believe the proposed revisions will lead to improved reliability, CenterPoint Energy is not necessarily opposed to revising CIP-002 to be a “bright line” criteria. However, CenterPoint Energy is concerned that ever-changing requirements represented by four versions of CIP-002 will add to the confusion of entities making good faith efforts to understand and comply with all the requirements embodied in the various CIP standards.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
LCEC	No	NERC distributed a questionnaire to responsible entities to gauge the impact of the proposed changes to CIP-002-4. The bright line criteria has changed since this assessment was performed and will result in the inclusion of additional assets being categorized as Critical Assets. Existing studies prove that many of these assets are not Critical Assets and do not impact the reliability of the BES. The existing CIP3 - CIP9 standards are not being modified with the version four release even though there are many opportunities to improve these standards. A good example can be seen with the Technical Feasibility Exception (TFE) process. Why are entities and regulatory agencies being forced to spend a significant amount of time processing TFE’s because requirements don’t make sense? A good example is the common TFE for routers and switches that do not and cannot run antivirus software. Expanding the scope of these labor intensive and non-value added processes will only deter entities from implementing effective security measures and best practices. A prudent

Organization	Yes or No	Question 1 Comment
		approach would be to adjust the bright line criteria to ensure that the assets being included in the scope of the version four standards are truly Critical Assets. Once the security control standards are improved, the scope can be expanded to include medium and low impact cyber systems.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology. The SDT agrees that other changes ultimately need to be made to the body of CIP cyber security standards, and expects to post them next year. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.		
Xcel Energy	Yes	We believe it has the potential to improve reliability by promoting consistency in the designation of critical assets.
Response: Thank you for your comments.		
Great River Energy	No	The Bright Line criteria will likely lead to the declaration of more critical assets. There is no way to judge whether this will lead to an improvement in reliability.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
ITC Holdings	Yes	It will bring consistency.
Response: Thank you for your comments.		
Public Utility District No. 1 of Clark County	Yes	The proposed CIP-002-4 standard adequately takes a major point of confusion out of the determination of Critical Assets by eliminating the reference to a risk-based methodology.
Response: Thank you for your comments.		
TransAlta		
Exelon	Yes	
AECI	Yes	

Organization	Yes or No	Question 1 Comment
N.W. Electric Power Cooperative, Inc.	Yes	
Central Electric Power Cooperative	Yes	
Central Electric Power Cooperative	Yes	
M & A Electric Power Cooperative	Yes	
LCRA Transmission Services Corporation	Yes	
Sho-Me Power Electric Cooperative	Yes	
KAMO Power	Yes	
United Illumiinating	Yes	We support the brightline approach
Response: Thank you for your comments.		
Constellation Energy Commodities Group	Yes	The attempt at additional clarity should assist in the identification of critical assets and is in support of FERC Order 706 paragraph 236.
Response: Thank you for your comments.		
Associated Electric Cooperative, Inc.	Yes	
KAMO Electric Cooperative	Yes	

Organization	Yes or No	Question 1 Comment
Northeast Missouri Electric Power Cooperative	Yes	
NW Electric Power Cooperative, Inc.	Yes	
Sierra Pacific Power d/b/a NV Energy	No	While the new proposed CIP-002-4 will provide more clarity to responsible entities about which Assets are deemed "Critical", this will not necessarily lead to any improvement in reliability. It sweeps in facilities that would, under most reasonable RBAM applications, be deemed non-Critical, and imposes security requirements that may be of little or no value. For example, there are numerous 345kV stations whose destruction would result in no material reliability consequence to the surrounding BES, yet under this proposal, these stations are Critical by prescription.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Sho-Me Power Electric Cooperative	Yes	
SDG&E	Yes	Comments: SDG&E generally agrees with the above statement to the extent that new assets may be identified that were not previously and to the extent the added comments submitted are considered.
Central Lincoln	No	As presently written, it may unintentionally bring in low/no impact equipment, thereby degrading reliability by spreading resources too thinly. We believe the SDT is on the right track, though.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Northeast Missouri Electric Power Cooperative	Yes	
National Rural Electric Cooperative Association (NRECA)		The mapping document is not an important part of the draft CIP-002-4 standard and does not have an impact on NRECA's view of the standard.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment.		
Tampa Electric	Yes	
M&A Electric Power Cooperative	Yes	
MEAG Power	No	There are system reliability projects with greater priority that will improve reliability more than a project implementing the proposed CIP-002-4 standard. If funding is taken away from the projects, BES reliability will be worse.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Associated Electric Cooperative, Inc.	Yes	
Associated Electric Cooperative, Inc.	Yes	
FirstEnergy Corp	Yes	FE believes the increased consistency offered through Attachment 1 will likely provide greater coverage of BES transmission assets. Whether or not there is a reliability improvement gain for the bulk electric system will depend on whether or not there are cyber devices as the Critical Assets now included by the bright-line methodology.
Response: Thank you for your comments.		
Minnesota Power	Yes	Minnesota Power believes that the adoption of a uniform and consistent methodology for the selection of Critical Assets will enhance the reliability of the bulk power system. However, as posted, the revised CIP-002-4 R3 makes two references to the “risk-based assessment methodology”. A risk-based assessment methodology is no longer applicable under the other requirements of CIP-002-4; therefore these references in CIP-002-4 R3 should be removed.
Response: Thank you for your comments. Prior to the next ballot, this reference will be removed.		
Manitoba Hydro	No	The question is difficult to answer in such a broad context. The improvement in reliability due to a change in

Organization	Yes or No	Question 1 Comment
		Critical Asset identification is unknown.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
American Transmission Company	Yes	ATC believes the adoption of a uniform and consistent methodology for the selection of Critical Assets will enhance the reliability of the BES.
Response: Thank you for your comment.		
Ameren	No	We believe that the proposed bright line criteria would provide uniformity and consistency in determining the critical assets by the registered entities. However, we do not believe that it will lead to an improvement in reliability for the following reasons: (1) The proposed bright line criteria are not based on any studies or performance testing. (2) The proposed bright line criteria do not address proximity to load centers or the impact to system flows or voltages in those load centers. Further, the bright line criteria will include many more facilities as critical assets with minimal to no improvement to reliability and would require significant resource commitment to meet in the proposed implementation plan time line.
Response: Thank you for your comments. (1) The SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. Significant feedback from the industry was the need to simplify the Critical Asset identification approach. We welcome your suggestions for improvement to the criteria. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The results of the recent NERC data request were used to assist the team in developing the criteria in Attachment 1. (2) Bright line criteria by its very nature may overreach in some areas and under reach in others, with the end result being a more protected system on average.		
BGE	Yes	Procedure is now clarified and will identify more critical assets that should improve system reliability.
Response: Thank you for your comment.		
Beaches Energy Services (of City of Jacksonville Beach, FL)	Yes	However, significant improvements can be made to Attachment 1, as described in my response to Question 2.
Response: Thank you for your comment. Please refer to response to comments in Question 2.		

Organization	Yes or No	Question 1 Comment
We Energies	Yes	We understand that the errata, which removes discussion of the "risk-based assessment methodology" from the proposed CIP-002-4 standard, would also apply to the mapping document. We appreciate the bright-line clarification to ensure consistent identification of Critical Assets throughout the industry.
Response: Thank you for your comment.		
City Utilities of Springfield, MO	Yes	City Utilities of Springfield, Missouri (SPRM) appreciates the work of the drafting team and welcomes the change to a standard that will state what the Critical Assets are and take away the ongoing debate. SPRM likes the idea of bright line criteria. It is a much simpler method to apply. SPRM believes this will potentially "lead to an improvement in reliability compared to the standard it proposes to replace." It does appear that the standard will increase the number of Critical Assets by arbitrarily declaring that all assets of a certain type are Critical Assets e.g., 1.4., 1.5., 1.6., 1.7., 1.11., 1.13. and 1.14. But does that mean that BES reliability has really improved or have we just created more administrative tasks that are unnecessarily burdensome to both Regional Entities and Registered Entities? We continue to support the suggestions offered by the APPA Task Force and others during previous comment periods that a risk assessment based on engineering studies would provide a more accurate listing of the truly critical assets. It appears that some of the criteria in Attachment 1 have the potential to meet that objective e.g., 1.3., 1.8., 1.9., 1.10., 1.12. Therefore, SPRM has decided to vote negative on this ballot and hopes the drafting team will consider our comments.
Response: Thank you for your comments. Please refer to the comments in Question 2.		
National Grid	Yes	First, the proposed standard will lead to an improvement in reliability for entities that are either newly registered or envision new assets coming under their CIP purview. However, based on a preliminary assessment, National Grid anticipates minimal impact of the proposed revisions for National Grid's registered entities. Because National Grid's current risk-based methodology for identifying critical assets is similar to the bright-line criteria proposed in the revision for CIP-002, National Grid's current critical asset list is very inclusive Hence, from National Gird's perspective, the proposed standard will not lead to a significant improvement in reliability with regard to National Grid's facilities because it will not result in a significant increase in the number of assets identified as critical. Second, the proposed revision to the standard aims to replace the existing risk-based methodology with the new bright-line criteria. However, R3 of the proposed standard (reproduced below) still refers to the risk-based methodology. National Grid proposes to delete the reference to the risk-based methodology in R3 for consistency and to reduce the possibility of confusion on the part of senior managers attempting to comply with R3.
Response: Thank you for your comments. Prior to the ballot, the reference to risk-based methodology in R3 will be removed.		

Organization	Yes or No	Question 1 Comment
Lincoln Electric System	No	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS). In addition, LES believes determining critical assets without the use of engineering studies severely limits the effectiveness of the exercise, especially when you consider this is an industry built substantially on engineering studies. A bright line approach may make it easier to identify critical assets, but that should not be confused with an improvement in accuracy. We believe an engineering study based assessment can result in the most accurate list of critical assets, in turn allowing us to truly improve system reliability by focusing the bulk of our efforts on protecting the assets that are truly critical.
Response: Thank you for your comments. Please refer to our response to MRO NERC Standards Review Subcommittee. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Southwest Power Pool Regional Entity	Yes	The addition of the Bright Line, while not perfect, gives certainty and uniformity to the identification of Critical Assets. The ambiguity and inconsistency brought by the entity-devised risk-based assessment methodology has been removed.
Response: Thank you for your comments.		
Indianapolis Power & Light	Yes	
Constellation Power Generation	Yes	Since no space was offered to accept comments on the applicability section, we offer some additional remarks in this section. There is no recognition within CIP2-004 of FERC's conclusion that only equipment not regulated by the U.S. Nuclear Regulatory Commission ("NRC") is subject to compliance with the CIP Reliability Standards. See Order 706-B, P. 1 and P. 7. In Order 706-B, FERC stated that "the Commission finds that the CIP Reliability Standards are applicable to all equipment within a nuclear power plant located in the United States that will not be subject to NRC's cyber security regulations." P. 7. In order to clarify the applicability of CIP2-004, Constellation Power Generation suggest adding the following language to the exemption section of the standard:4.2.2 Cyber Assets associated with Cyber Security Plans submitted to the U. S. Nuclear Regulatory Commission pursuant to 10CFR73.54.Cyber security regulations applicable to nuclear power plants are set forth in 10CFR73.74, as was noted by FERC. Order 706-B at fn. 6. These regulations are final and currently effective. This exemption language should be added to CIP-003 thru -009 as well.
Response: Thank you for your comments. The Applicability section has been revised to address nuclear plants.		

Organization	Yes or No	Question 1 Comment
Independent Electricity System Operator	No	We do not believe the standard will result in an improvement in reliability since the revisions merely replace the risk-based assessment methodology with a list of criteria that will ultimately result in inclusion of facilities on the Critical Assets list that are non-impactive on the BES.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
American Electric Power (AEP)	No	See comments for the questions below. Furthermore, This standard does not address the in process brightline jurisdictional work between the NRC and NERC as part of 706b. We suggest to the SDT that some consideration be made to referencing those activities.
Response: Thank you for your comment. The Applicability section has been revised to address nuclear plants.		
Orlando Utilities Commission	Yes	
Oglethorpe Power Corporation	No	CIP versions 1-3 allow each entity to follow their own Risk Based Assessment Methodology, which could lead to an inconsistent application of the standards across the continent. CIP version 4 seeks to avoid this potentially inconsistent application by providing so-called “bright line” criteria which must be used by all Registered Entities to define their Critical Assets. While this version certainly succeeds in a uniform application of the standards across all Registered Entities, it is impossible to say whether this will result in a more reliable system for the following reasons:1. It is unknown whether the new criteria will lead to the inclusion of additional Assets or the exclusion of existing Assets in the Critical Asset list and more importantly,2. It is also unclear whether the new list of Critical Assets will include additional assets that affect the reliability of the system in a material way or whether some Assets which do affect the grid may now be excluded.3. It is still unclear how great a threat to reliability cyber threats really are and4. It is unknown how well the remaining CIP standards mitigate that threat.
Response: Thank you for your comments. 1.: The SDT believes that the implementation of Attachment 1 criteria will not only result in a more uniform identification of assets but will also result in a larger number of Critical Assets being identified in North America. 2.: Bright line criteria by its very nature may overreach in some areas and under reach in others, with the end result being a more protected system on average. 3. The utility industry has been addressing reliability from a contingency perspective for many years and has a good understanding of this analysis. Cyber security protection must consider possible malicious compromise of multiple assets (not just loss), where expected outcomes can have significantly more impact than single contingency outages. 4. The CIP standards provide a set of well known good security practices that are considered a minimum level of protection against potential cyber threats.		
Brazos Electric Power	No	The proposed standard will improve clarity for documentation and audit purposes but it does not necessarily

Organization	Yes or No	Question 1 Comment
Cooperative, Inc.		leads to improvement in reliability.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology.		
Midwest ISO	No	While changing this standard to bright line criteria does make it easier to understand when an asset is critical and makes the standard easier to enforce, it is unlikely to result in an improvement in reliability. Protecting the electric industry's portion of the national infrastructure is a complicated and challenging problem that requires a complex solution. While applying bright line criteria may represent an easily understandable solution, it does not represent the complex solution that this problem requires. Thus, the criteria will likely result in assets being selected as Critical Assets when they are not truly critical and assets that are truly critical not being selected as Critical Assets. It is even possible that it could result in a net decrease in assets covered. Even if there is a net increase in assets covered, the assets are in all likelihood already protected against cyber threats for business reasons.
Response: Thank you for your comments. The SDT believes that the implementation of Attachment 1 criteria will improve reliability through greater consistency of Critical Asset identification over the existing entity defined risk-based methodology. Bright line criteria by its very nature may overreach in some areas and under reach in others, with the end result being a more protected system on average. While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets in North America will be classified as Critical Assets.		
Duke Energy	Yes	However, CIP-003 through CIP-009 need modifications other than just changing the revision numbers, as evidenced by numerous interpretation requests and general confusion in the industry. While we understand that the plan is to complete those modifications in 2011, industry will be adding numerous Critical Assets and Critical Cyber Assets due to these revisions to CIP-002. Applying the current versions of CIP-003 through CIP-009 to numerous additional Critical Cyber Assets compounds the difficulty of maintaining compliance without more clear direction.
Response: Thank you for your comments. The SDT agrees that other changes ultimately need to be made to the body of CIP standards, and expects to post them next year.		
Seminole Electric Cooperative, Inc.	No	
Progress Energy	Yes	
Orlando Utilities Commission	Yes	

Organization	Yes or No	Question 1 Comment
New York Independent System Operator		
Cowlitz County PUD	Yes	However, as written it is too inclusive. Cowlitz believes the attachment to the standard will draw in more than just the High Impact categories. Facilities categorized as Critical Assets in CIP-002-4 should not later be categorized as Medium or Low Impact after implementation of CIP-010 and CIP-011. Please refer to APPA comments; suggested changes to the attachment: 1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer.; 1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria: 1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW; 1.7. Each Transmission Facility operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher where the TPL peak load studies of the Planning Coordinator or Transmission Planner identifies the sum of the incoming power flows or the sum of the outgoing power flows to exceed 1500 MW; 1.8. Transmission Facilities at a single station or substation that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs) as determined by the Reliability Coordinator; 1.13 Common control system(s) configured to perform automatic load shedding of 300 MW or more within 15 minutes; 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control; 1.15 Each control center or backup control center used to control multiple generation units identified as Critical Assets designated under criterion 1.3 or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.
Response: Thank you for your comments. Please refer to the comments in Question 2.		
Orlando Utilities Commission	Yes	
Kansas City Power & Light	No	Absent engineering analysis and study, the proposed changes and bright line established in this Standard does not ensure an improvement to system reliability. It is possible this proposed Standard will impose additional obligations to protect assets that do not contribute to ensuring the reliability of the bulk electric system taking resources of time and money to support compliance efforts to meet these proposed requirements and taking those resources away from other efforts that could have a positive impact on improving bulk electric system reliability.
Response: Thank you for your comment. Bright line criteria by its very nature may overreach in some areas and under reach in others, with the end result being a more protected system on average.		

2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Summary Consideration: In response to question 2, most commenters had suggestions for improvement to the criteria for critical assets listed in Attachment 1. The SDT appreciates these comments and incorporated many of them to improve clarity and consistency. Some of the comments reflected a misunderstanding of a specific criterion, and in those instances the SDT provided additional guidance in the response to comments and modified the associated guidance document for identifying Critical Assets. The SDT believes that the implementation of Attachment 1 criteria will increase the overall consistency of Critical Asset identification. Specific summary analysis of each criterion follows, along with a summary of responses.

Criterion 1.1 defines as Critical Assets "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW." Commenters requested clarification on "single plant location." Clarity on this issue was provided in the posted guidance document. Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant. Other commenters questioned why we no longer used Contingency Reserve in the criteria, and how the SDT arrived at the value of 1500 MW. In prior postings of CIP-002-4 and CIP-010-1 there was wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The SDT performed an informal survey of the regions and identified what the megawatt value of the reserve sharing would be for various groups. The SDT used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions. Some commenters suggested the use of capacity factor in the criterion. The SDT debated whether to include capacity factor in this criterion. The reason the SDT ultimately chose not to include capacity factor is twofold. There is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. There was also a concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year. After considering all of the comments, the SDT chose not change the wording of criterion 1.1.

Criterion 1.2 defines as Critical Assets "Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater." Some commenters questioned how the value of 1000 MVARs was derived. The value of 1000 MVARs used in this criterion was deemed reasonable for the purpose of determining criticality. Some commenters suggested combining criterion 1.2 with criterion 1.9. FACTS devices in 1.9 are specifically related to IROLs, whereas the reactive resources in 1.2 are not limited to IROL applications. Some commenters suggested that the limit should be set by each Regional Reliability Organization. The issue with using different MVAR values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. After considering all of the comments, the SDT chose not change the wording of criterion 1.2.

Criterion 1.3 defines as Critical Assets "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." Many commenters felt that this criterion places the responsibility for identifying

the asset with the wrong entity (not the asset owner). Other commenters noted that the use of the NERC Glossary term "Adverse Reliability Impacts" would help clarify which units should be in this category. Others expressed concern that the criterion should mandate the coordination and approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. Still others stated that this criterion is open for auditors to interpret. The SDT responded that the burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability. Based on the comments received, this criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Criterion 1.4 defines as Critical Assets "Each Blackstart Resource identified in the Transmission Operator's restoration plan." Many commenters expressed concern that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. Others stated that blackstart units deemed critical should be only those identified by the TOP as specified to meet the minimum critical blackstart requirement. Some expressed concern that criterion 1.4 inadvertently provides incentive to utilities to remove resources from the restoration plan, reducing the plan's overall effectiveness. The SDT specifically chose the NERC Glossary term "Blackstart Resources" to address the concerns expressed. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. After considering all of the comments, the SDT chose not change the wording of criterion 1.4.

Criterion 1.5 defines as Critical Assets "The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist." Some commenters stated that additional qualifying criteria should be added such as "Cranking Paths to critical units as identified in a region's restoration plan." The SDT noted in its response that there is no longer any NERC requirement to have a region restoration plan. Others asked for clarity around where the point of multiple paths lies in the electrical system. The SDT noted in its response that the point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. Some commenters expressed concern over the phrase "initial switching requirements." Based on the comments received, this criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first

interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan."

Criterion 1.6 defines as Critical Assets "Transmission Facilities operated at 500 kV or higher." Commenters expressed that voltage alone is not a sufficient criterion to determine whether or not an asset is critical to the bulk electric system. They suggested that the SDT should consider using capacity or flows based on power flow studies instead of nominal voltage level as the bright line. The SDT responded that all Transmission Facilities operated at 500 kV or higher do not require any further qualification for their role as components of the backbone on the Interconnected BES. Furthermore, the SDT does not feel that capacity or power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. The SDT will take this suggestion under consideration for future revisions. After considering all of the comments, the SDT chose not change the wording of criterion 1.6.

Criterion 1.7 defines as Critical Assets "Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations." Some commenters provided the suggestion that criterion 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations). Others commented that the SDT should adopt a power flow based bright-line rather than whether the station is connected to three or more other stations, similar to comments for criterion 1.6. Again, the SDT does not feel that power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. Still others commented that the statement regarding "three or more other transmission stations" is confusing. Does the criterion include stations upstream, downstream, networked or radial? Does the criterion include a radial 345 kV substation connected to a generator? The SDT response is that the intent of criterion 1.7 is to classify as Critical Assets all Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this criterion, since the criterion specifically states "three or more other transmission stations." The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. Based on the comments received, this criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."

Criterion 1.8 defines as Critical Assets "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Some commenters stated that this criterion should be modified because loss of facilities does not cause an IROL violation. An IROL includes a limit and a time constant T_v. In order for an IROL violation to occur, the limit must be exceeded for at least the time constant T_v. Others commented that additional language should be added to clarify that the TO, LSE, etc. is not responsible for demonstrating IROLs. The SDT responded that according to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. Based on the comments received, this criterion has been reworded to "Transmission Facilities

at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Criterion 1.9 defines as Critical Assets "Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Some commenters felt that the term FACTS should be added to the NERC Glossary. FACTS is defined by IEEE as: "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Commonly accepted terms and definitions do not require an insertion in the NERC Glossary. Some questioned why FACTS devices were singled out in the criteria. FACTS devices were singled out to ensure that there was no confusion as to whether or not they were considered Critical Assets. Other comments followed a similar vein as criterion 1.8. Based on the comments received, this criterion has been reworded to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Criterion 1.10 defines as Critical Assets "Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3." Some commenters asked for clarity about the term "directly connected." Additional questions concerned whether the language means total loss of a substation or only partial. The intent of this criterion is to ensure the availability of Facilities necessary to support generation Critical Assets. Any Transmission Facility the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. This might include the partial or total loss of a substation. Based on the comments received, this criterion has been reworded to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."

Criterion 1.11 defines as Critical Assets "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements." Some commenters stated that criterion 1.11 should be eliminated on the basis that is not based upon BES reliability considerations and that criticality of facilities should not be fuel specific. Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC reliability standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. Some felt that this criterion should be limited to Transmission Facilities providing offsite power requirements. Since NUC-001-2 is not limited to offsite power requirements, it did not seem appropriate to limit this criterion. After considering all of the comments, the SDT chose not change the wording of criterion 1.11.

Criterion 1.12 defines as Critical Assets "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate

one or more Interconnection Reliability Operating Limits (IROLs)." Comments similar to those for criterion 1.8 concerning IROLs were received on this criterion. Based on the comments received, this criterion has been reworded to "Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed."

Criterion 1.13 defines as Critical Assets "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes." Some commenters stated that the wording of this criterion will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. Still others stated that this criterion should use the same "bright line" as generation, 1500 MW. This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. Based on the comments received, this criterion has been reworded to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Criterion 1.14 defines as Critical Assets "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." No commenter stated that this criterion was inappropriate for Reliability Coordinators. Several commenters stated that the term "control center" needs to be defined in the NERC Glossary. At this time, the SDT is choosing not to add control center to the NERC Glossary. It was felt that defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. Many commenters stated that control centers for Balancing Authorities (BA) and Transmission Operators (TOP) need bounds. It was stated that a small BA or TOP that does not have any other Critical Assets does not need all of the Requirements in CIP-003-4 to CIP-009-4 applied to them. After considerable discussion, it was determined by the SDT that these "small" BAs and TOPs could be addressed in the next version of the standard. Based on the comments received, this criterion has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 (the posted criterion 1.16 has been removed, see explanation below) has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

Criterion 1.15 defines as Critical Assets "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Comments received on this criterion were similar to those received on criterion 1.1 and criterion 1.14. Based on the comments received, this criterion has been reworded to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MWs in a single Interconnection."

Criterion 1.16 defines as Critical Assets "Any additional assets that the Responsible Entity deems appropriate to include." This criterion was placed in Attachment 1 to provide Responsible Entities the flexibility to include addition items on their Critical Asset list that did not meet any other criterion in Attachment 1. Many commenters stated that this was contrary to providing a bright line for Critical Asset identification. In addition, it has the potential of causing issues in compliance audits. For these reasons, criterion 1.16 in its current form was deleted from Attachment 1.

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	Yes	Item 1.1: 1500 MW is too high a value that will not capture a significant number of large generation assets which are needed for reliability. 300 MW is a more realistic value consistent with a similar impact that Load Serving Entities have in Item 1.13. Recommend revised language, "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 300 MW." Item 1.3 "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." This latest version of the CIP Standard establishes that "the Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria." Therefore, Item 1.3 appears to establish that if a PC/TP designates a generation facility as "required for reliability purposes", the Registered Entity shall determine that the generation facility is an identified Critical Asset. This Item must be struck from Attachment 1 for numerous reasons. First, the current version of Item 1.3 has the same problems as the proposal to include "reliability must run" in the Criteria and, in an even earlier draft, to assign responsibility to a so-called "Reliability Assurer". As many commented in prior drafts of the CIP Standard, Criteria like that proposed for Item 1.3 are undefined and places the responsibility for identifying the asset with the wrong entity. Specifically: (a) unlike the other Items in the Attachment, Item 1.3 lacks specificity required for providing registered entities with clear guidance on which assets should be deemed critical under CIP-002. Even if the PC/TP were the correct party for making such identifications (which it is not), the Item contains no guidance on how to make such determinations. (b) By placing the PC/TP in the responsible position for identifying which assets are needed for reliability, the Item conflicts with Order No. 706 (as explained further below), stating that the Registered Entity is responsible for identifying their own critical assets. FERC has

Organization	Yes or No	Question 2 Comment
		stated that the Registered Entities which own the assets are responsible for identifying their assets, and that they should receive guidance from NERC. Item 1.3 does not contain such guidance. (c) Furthermore, with the way Item 1.3 is structured in the Attachment, it also is likely to have the effect of disincentivizing Registered Entities from analyzing whether their own assets are critical, as they are likely to simply wait to be notified from their PC/TP as to whether they are needed for reliability. Even if Item 1.3 is meant only to apply to a Planning Coordinator/Transmission Planner doing "exception-type" reviews, including this role in the Standards suggests that so long as a Responsible Entity does any type of engineering evaluation, the Responsible Entity can effectively shift responsibility to the external reviewer. Because there is no sanction for incomplete or non-substantive evaluations, the Planning Coordinator/Transmission Planners may be deluged with requests to "exempt" assets from the Attachment 1 categorization. This language would effectively undermine FERC's direction that Responsible Entities remain responsible for classifying their assets and they cannot shift this responsible to the Regional Entity or another Organization. See Order No. 706 at P328. (d) the item fails to provide necessary guidance in that it does not guide the PC/TP as how to assess what risks to take into account for making its determination about whether the facility is "required for reliability purposes". This is especially problematic given the views that cyber-attacks are intentional and malicious in nature and NERC's position that N-1 criteria is not a sufficient basis for determining which assets need to be protected for CIP Standards. See "Critical Cyber Asset Identification", Memo from Michael Assante to Industry Stakeholders (dated April 7, 2009) (available at: http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf) Second, to the extent that the SDT and NERC desire, third-party review of a Registered Entity's determinations, that review should be handled through the NERC Rules of Procedure/CMEP, and not in the Standard Requirements. The key parts of Order No. 706 (and 706-A) set out three (3) principles.(I) Responsible entities are, and should remain, responsible for identifying their own assets as requiring critical infrastructure protection. The SDT makes clear in the plain language of the Standard that Responsible Entities are responsible for their own assets. Paragraph 328 of Order No. 706 states that: "responsibility for identifying critical assets should not be shifted to the Regional Entity or another organization instead of the applicable responsible entities identified in the current CIP Reliability Standards. As we stated in the CIP NOPR, and confirmed by commenters, such a shift would not improve the identification of critical assets, but would likely overburden the Regional Entities. While we are sympathetic to AMP Ohio's concerns regarding small generation owners, generation operators and load serving entities that have a limited view of the Bulk-Power System, we believe that NERC's development of guidance on the risk-based assessment methodology and our direction above to provide assistance to small entities should support the efforts of entities - both small and large - in performing a proper assessment. We do not believe that the lack of a wide-area view is sufficient reason to forego an assessment or taking responsibility." See also Order No. 706-A at P53 (: "The responsibility for properly identifying all of a responsible entity's critical assets and critical cyber assets and adequately protecting those assets rests firmly with the responsible entity. The fact that the Commission has directed the ERO to develop an external review process - as a backup to help assure that the responsible entity does not overlook any critical assets - does

Organization	Yes or No	Question 2 Comment
		not shift this responsibility from the responsible entity to whatever entity conducts the external review.") (II) NERC and the Regions should issue guidance to Responsible Entities that do not have a "wide-area" view in order to assist them in identifying which of their assets required critical infrastructure protection (Order No. 706 at P322). The SDT had provided guidance in the form of the Standard itself - i.e., Attachment 1. This Draft Standard effectively directs Registered Entities on how to classify their assets.(III) External review is necessary to: (a) help identify trends in the industry (Order No. 706 at P322 and to support consistency (Id.), and is necessary to review asset more frequently than would occur through the regular audit cycle. (Order No. 706 at P324) (FERC "does not believe that the audit process will provide timely feedback to a responsible entity regarding critical asset determinations"). FERC has explained that NERC may choose to "designate" a Registered Entities (such as, but not necessarily, a Reliability Coordinator) as responsible for this external review if NERC/Regional Entities determined that they did not have the resources/expertise to conduct this review. (Order No. 706 at P255)("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). In Order No. 706-A, FERC added that if NERC designated a Reliability Coordinator as having oversight/review authority, the Reliability Coordinator should have the same liability protections as NERC. (Order No. 706-A at P53).In drafting CIP-002-4, Item 1.3 takes a wrong approach to addressing the Commission's concerns in Order No. 706. With regard to the need for more frequent external review than that provided by audits can and should be handled outside of the Standard Development Process. For example, NERC and the Regions can establish spot-checks or off-site audits through the CMEP program, and NERC can require Responsible Entities to submit information to it (or the Regions) through an information request developed under its Rules of Procedure. If the SDT and NERC address the role of third party review through NERC's administration of its Rules of Procedures, many significant problems with Item 1.3 would be eliminated. These problems are summarized below.It is premature to place "Planning Coordinators/Transmission Planner" in the Standard. Because NERC has not found that it lacks sufficient resources to take on the external review responsibility, and thereby has not "designated" any other type of Registered Entity with this responsibility, it is premature for the Standard to make reference to the Planning Coordinator/Transmission Planner. See Order No. 706 at P255 ("[w]hile we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review

Organization	Yes or No	Question 2 Comment
		of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System"). If the Standard Drafting Team is committed to including in its Standard reference to a Registered Entity as having external review oversight, it should wait until NERC makes its designation.Assigning external review responsibilities to Planning Coordinators/Transmission Planners, as opposed to Regional Entities, is likely to fail to achieve FERC's goal of consistency. Because NERC and the Regional Entities work closely as part of their Regional Entity Delegation Agreement, and because there are fewer Regional Entities than Reliability Coordinators, achieving consistency will be easier if the Regional Entities have the external oversight responsibility. Importantly, because the Standard offers no guidance to Planning Coordinators/Transmission Planners on how to determine if generation facilities are needed for reliability under CIP-002, consistency is unlikely to be achieved.Even if NERC "designates" a Registered Entity (such as, perhaps, the Planning Coordinator/Transmission Planner) as having a role in providing external review, the Registered Entity should have the same liability protections as NERC, as the Registered Entity is essentially carrying out this role as a NERC-designee. It is easier to capture the roles, responsibilities and liabilities protections through amendment to the Delegation Agreements and Rules of Procedure. In Order No. 706-A, FERC reaffirmed the protections given to external reviewers. See Order No. 706-A at P53 (""we agree [with the ISO/RTO Council] that entities designated by the ERO to perform reviews of a responsible entity's critical asset list should receive the same liability protection for performing this review that the ERO or Regional Entity would have if it performs this review itself."). These protections include no finding of liability unless intentional misconduct or gross negligence is found. See, e.g., Bylaws at Section 3 (NERC's trustees, officers, employees, and agents are held harmless "for any injury or damage to [any NERC Member] caused by any act or omission of any trustee, officer, employee, agent, or volunteer in the course of performance of his or her duties on behalf of the Corporation, other than for acts of gross negligence, intentional misconduct, or a breach of confidentiality"). In sum, the SRC recognizes that a different set of expectations may apply to those Regional Entities that are also Registered Entities (e.g., WECC). These entities already have liability protections per their NERC delegation agreements, and in their role as Regional Entities, they ultimately have authority over whether the Responsible Entity has correctly identified bulk power system assets as subject to critical infrastructure protection. Similarly, some of the Canadian Reliability Coordinators (e.g., IESO through its enforcement group) exercise similar oversight authority as a Regional Entity with regard to other Registered Entities. The Critical Assets listed in 1.6 and 1.7 would have the undesired result of having facilities included that will have no impact on BES reliability. The list of applicable facilities should be determined following an impact-based assessment to be performed by the Reliability Coordinator. If necessary, an additional requirement for the RC to have a risk-based assessment methodology, and to conduct/review the assessment should be included. Suggest 1.6 and 1.7 be reworded as follows:1.6 Transmission facilities operated at 500kV or higher, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability,

Organization	Yes or No	Question 2 Comment
		separation, or cascading outages.1.7 Transmission Facilities operated at 300 kV or higher to less than 500 kV at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages. Item 1.15: Size should not be a consideration when determining CA criteria for control centers, control systems, backup control centers and backup control systems used to control generation. Recommend removal of this item and add Generation Operator to this list of functional entities included in Item 1.14. General: Due to the interconnected nature of responsible entities as well as the downstream requirements of entities to act on information from another party, the listing in Attachment 1 does not adequately address the risk that an entity poses to another entity. For example, not all control centers with ICCP connectivity to RC/BA/TOP are required to be categorized as Critical Assets. Paragraph 256 of FERC Order 706 highlights the issue in this oversight. "A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset." It should further assert that the protection should be afforded to those connected to the asset or relying on information from the asset to facilitate real-time operations.Include the class of assets - generation, transmission, and control centers against each criterion in Attachment 1. This will help entities to clearly identify which requirements fall under different classes of assets. For example - 1.5 The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. (Generation, transmission)

Response: Thank you for your comments.

Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The drafting team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Based on information provided on the DOE website, the SDT believes that an increased amount of generation capacity will be classified as Critical Assets in the US.

Item 1.3 – The burden for identifying Critical Assets resides with the Responsible Entity that is the asset owner. The Planning Authority and/or Transmission Planner are not designating the asset as critical for CIP purposes; they are determining the unit to be necessary to avoid Adverse Reliability Impacts based on other NERC reliability standards. This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Organization	Yes or No	Question 2 Comment
Items 1.6 and 1.7 – You propose to add the criteria that the RC can determine through a risk based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The inclusion of a risk-based evaluation by any entity would not meet the objective of uniform application of Critical Asset identification across all entities. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.15 – This designates generation control centers that control generation Facilities as Critical Assets or used to control generation greater than an aggregate of 1500 MW in a single Interconnection as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. General –The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the administrative impact on the industry while addressing the identified consistency issues. The drafting team agrees that the issue of Cyber Security and Cyber Security protection is extremely complicated. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The team expects to continue its work on a functional approach after Version 4.		
City of Garland	Yes	Attachment 1 - 1.15 states "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection". Blackstart Units are identified as Critical Assets in Attachment 1 - 1.4. During Blackstart situations, the Blackstart unit is under the direction / control of the Transmission Operator (TOP). The Blackstart unit IS NOT under direction / control of the Generator Operator (GOP) or under the control of the GOP's dispatch control system during the Blackstart condition. Therefore, the GOP's dispatch control system should not be forced to be classified as a Critical Asset due to a Blackstart unit which the GOP has no control over during a Blackstart situation.
Response: Thank you for your comments. Item 1.15 – The concern here is that the GOP control center could provide a path to compromise the functionality of the Blackstart Resource.		
NRG Energy Inc.	Yes	1.1 - Add capacity factor as a qualifier for exclusion below an established low threshold. 1.3 - Mandate coordination/approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. These classifications and approvals need to take into consideration 5 year forecasts for planning and budgeting purposes.. 1.5 - TOP needs to define the cranking path in restoration plan to the affected entities to adequately secure these restoration paths.. 1.9 - Please explain FACTS - need definition

Organization	Yes or No	Question 2 Comment
		1.10 - Need coordination between TOP & GO to identify critical assets. 1.15 - How is the 1500 MW aggregate determined? Is it an aggregate of generator name plates or the sum of controllable megawatts between a unit's high and low limits? General: Attachment 1 needs to have defined terms for capability, plant, control center

Response: Thank you for your comments.

Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. There is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. There was also a concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability.

Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan." This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.9 – FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability."

Item 1.10 – The assets would be identified by the asset owners. It is agreed that communication between GOs and TO/TOPs will be required. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."

Item 1.15 – This is the aggregate highest rated net Real Power capability output of all generation under dispatch/control.

At this time, the SDT is choosing not to add capability, plant or control center to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in

Organization	Yes or No	Question 2 Comment
effect.		
APPA CIP-002-4 Task Force	Yes	SDT Proposed:1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. APPA Comments: APPA and others commented on the CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. APPA commends the SDT for their attempted to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. The use of an average of the Contingency Reserve numbers from all the regions bases the bright-line on what the regions consider operationally significant. We understand that NERC standards are a minimum requirement and regions can look at their own operating criteria and determine if they need additional protection at lower Megawatt bright-lines. APPA is concerned that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2.R2. The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities. SDT Proposed:1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. APPA Comments: APPA does not have a comment on criteria 1.2 at this time. SDT Proposed:1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes. APPA Comments: APPA commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. APPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: "Adverse Reliability Impacts" will help clarify which units should be in this category. We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. APPA proposes the following rewording of criteria 1.3:"1.3 Each generation Facility that the Planning Coordinator or

Organization	Yes or No	Question 2 Comment
		Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer." SDT Proposed:1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. APPA Comments: APPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). APPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, APPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW. We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan. We further support inclusion of "ALL Blackstart Resources" when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal. SDT Proposed:1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. APPA Comments: APPA commends the SDT on differentiating between a single Cranking Path as a critical

Organization	Yes or No	Question 2 Comment
		facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. APPA does request clarification of criteria 1.5: Where does this point of multiple paths lay in the electrical system? Does this include only the Generator Step-up Transformer, or does it include the whole substation where multiple transmission paths depart to a single generator? Also, APPA suggests that the SDT change “switching requirements” to “switching equipment.” SDT Proposed:1.6. Transmission Facilities operated at 500 kV or higher. APPA Comments: APPA does not have a comment on criteria 1.6 at this time. SDT Proposed:1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. APPA Comments: APPA believes that criteria 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations).APPA also supports the MRO standard review team proposal to adopt a power flow based bright-line rather than whether the station is connected to three or more other stations: Under TPL-001, the Planning Coordinator or Transmission Planner already performs annual near-term power flow assessment and this particular assessment would be based on the forecasted peak conditions using Category A of Table 1 of the standard. Proposed rewording of criteria 1.7:1.7. Each Transmission Facility operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher where the TPL peak load studies of the Planning Coordinator or Transmission Planner identifies the sum of the incoming power flows or the sum of the outgoing power flows to exceed 1500 MW. SDT Proposed:1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). APPA Comments: APPA believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). We also request that it be clarified who will determine the IROL’s using similar wording to FAC-014: “R5. The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits...”Proposed rewording of criteria 1.8:1.8. Transmission Facilities at a single station or substation that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs) as determined by the Reliability Coordinator. SDT Proposed:1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability

Organization	Yes or No	Question 2 Comment
		Operating Limits (IROLs). APPA Comments: APPA believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). SDT Proposed:1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3. APPA Comments: APPA does not have a comment on criteria 1.10 at this time. SDT Proposed:1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements. APPA Comments: APPA does not have a comment on criteria 1.11 at this time. SDT Proposed:1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). APPA Comments: APPA understands there are utilities within the NPCC region that have SPS type 3 systems that only protect local areas. We seek verification from the SDT that the SPS they refer to in criteria 1.12 is for wide area protection only. SDT Proposed:1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. APPA Comments: APPA believes the SDT's change in wording of criteria 1.13 will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. As written, this criteria designates as a critical asset various control systems that by themselves could not cause instability or uncontrolled separation of the BES.APPA offers the following alternatives for rewording 1.13:1.13 Common control system(s) configured to perform automatic load shedding of 300 MW or more within 15 minutes. APPA can accept the bright-line of 300 MW if the wording is changed to that stated above, but we still see this bright-line as an arbitrary threshold based on a quantity that has no BES operational significance. Rather, 300 MW is a DOE threshold for electric event reporting. SDT Proposed:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. APPA Comments: APPA is concerned that criteria 1.14 is overly broad because it includes all BA and TOP

Organization	Yes or No	Question 2 Comment
		control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15. APPA offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. APPA cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability or uncontrolled separation of the BES. However, we will support inclusion of "ALL BA and TOP control centers" when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal. SDT Proposed:1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. APPA Comments: In the NERC Draft CIP-002-4 webinar it was stated that a control center in criteria 1.15 is understood to be controlling multiple units. APPA recommends that the SDT clarify the wording in criteria 1.15 to coincide with this understanding: 1.15 Each control center or backup control center used to control multiple generation units identified as Critical Assets designated under criterion 1.3 or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. SDT Proposed:1.16. Any additional assets that the Responsible Entity deems appropriate to include. APPA Comments: APPA believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Response: Thank you for your comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the

Organization	Yes or No	Question 2 Comment
Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.7 – The SDT agrees to change "stations" to "stations or substations." The SDT does not believe that power flow based bright-line criteria that is based on MW flows into or out of a substation would meet the objective of uniform application of Critical Asset identification across all entities. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 – The SDT agrees to change "stations" to "stations or substations." According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. The present wording is appropriate. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 - The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.12 – Since this item only applies to SPSs that have IROLs associated with them, local area SPSs are not included. This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11			

Organization	Yes or No	Question 2 Comment
or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 – This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
IRC Standards Review Committee	No	See comments to Question 1 above, and the proposed Attachment 1. (Below copied from question 1) The assets that should be subject to protection under the NERC CIP Standards should not be driven by the physical assets that are implicated in maintaining physical system reliability from an operations and planning perspective. There is not a direct relationship between assets that are subject to protection under the CIP standards and assets that form the basis for the current NERC understanding of planning and operating reliability. Nor should the scope of cyber assets be determined by the identification of physical asset by third parties. Under the current and proposed CIP Standards, the scope of jurisdictional cyber assets is driven by an entity's Critical Assets, which are physical assets that impact system reliability from an operations/planning perspective (i.e. Critical Assets are defined as: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.). In addition, the proposed standards include third party identification of critical assets. The Standards Drafting Team should take this opportunity to eliminate all of these inappropriate relationships. As an initial matter, the SDT should remove the term "Critical Assets" from the standard. This term should be replaced with a general term, such as "Assets Subject to Cyber Security Protection". This change will eliminate the inappropriate cause and effect relationship between physical system reliability - i.e. operations and planning - and cyber security. Instead, the general term directly links the driver of asset identification to cyber security. The next step should focus on the explicit identification of assets that fall within this category. The identification should be based on an objective list of assets. This mitigates the problems that arise from the application of a subjective identification methodology. Attached to these comments is a proposed list, which is intended to be used as a starting point (see proposed Attachment 1 below). The SRC believes this list includes asset types that should be subject to the CIP standards. However, at this point, the list is illustrative and is not intended to be exhaustive. This approach enables the identification of assets that are subject to cyber security protection irrespective of their relationship to the definition of "Critical Asset". By decoupling the assets subject to cyber protection from the subjective "Critical Asset" terminology, the proposed approach actually expands the number of assets that are subject to the CIP standards. This

Organization	Yes or No	Question 2 Comment
		approach is a relative improvement because it provides certainty to the regulated community and the regulators by removing the subjectivity associated with the use of terms such as “critical” or “reliability”. In addition to the above recommendations, the SDT should also revise Attachment 1 to explicitly clarify which functional entities are responsible for the relevant asset types. A revised version of Attachment 1 that reflects the above recommendations is provided below. CIP-002-4 - Attachment 1 Assets Subject to Cyber Security Protection The following are assets subject to Cyber Security Protection: 1. By the Generation Owner (GO): 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. 1.2. Each resource asset that the GO’s Planning Coordinator identifies that if that asset is destroyed, degraded, misused or otherwise rendered unavailable, will violate one or more Interconnection Reliability Operating Limits (IROLs). 1.3. Each Blackstart Resource identified in the GO’s Transmission Operator's restoration plan. 1.4. Each control center, control system, backup control center, or backup control system used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. 1.5. Each GO’s Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 2. By the Transmission Owner (TO): 2.1. Transmission Facilities operated at 500 kV or higher. 2.2. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. 2.3. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. 2.4. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. 2.5. Each resource asset that the TO’s Planning Coordinator identifies that if that asset is destroyed, degraded, misused or otherwise rendered unavailable, will violate one or more Interconnection Reliability

Organization	Yes or No	Question 2 Comment
		Operating Limits (IROLs). 2.6. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. 2.7. Each TO's Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 2.8. Transmission Facilities identified by a nuclear asset owner as essential to meeting Nuclear Plant Interface Requirements. 2.9. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.4. 2.10. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 3. By the Reliability Coordinator 3.1. Each control center, control system, backup control center, or backup control system used to perform the RC functional obligations 4. By the Transmission Operator 4.1. Each control center, control system, backup control center, or backup control system used to perform the TOP functional obligations 4.2. Each TOP's Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 5. Balancing Authority 5.1. Each control center, control system, backup control center, or backup control system used to perform the BA functional obligations
Response: Thank you for your comments. The drafting team agrees that the issue of Cyber Security and Cyber Security protection is extremely complicated. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The team expects to continue its work on a functional approach after Version 4. The SDT feels that the current format for Attachment 1 is sufficient.		

Organization	Yes or No	Question 2 Comment
Bonneville Power Administration	Yes	Make it clear that substations are the facilities to be identified as Transmission Critical Assets, not lines, transformers, reactive equipment, etc. Another alternative would be to identify all facilities that operate at a specified certain kV level would be determined to be Critical Assets. The different categories identified in Attachment 1 still allow utilities to justify most of what they have already declared as Critical Assets.
Response: Thank you for your comments. Substations are not the only Facilities identified as Critical Assets. Lines, transformers, reactive equipment, and other Facilities can be classified as a Critical Asset if they meet any of the criteria in Attachment 1. Please refer to the guidance document posted on the project page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf for additional clarification.		
PSEG Companies	Yes	In Attachment 1, item 1.4 the blackstart units deemed critical should be only those identified by the TOP as specified to meet the minimum critical blackstart requirement. The TOP may choose to list all its area blackstart capable units in its plan for informational purposes, but a subset of that list may be what is required for blackstart and only those should be considered critical. PSEG suggests that 1.4 be reworded as follows:"Each Blackstart Resource identified in the Transmission Operator's restoration plan required to meet the minimum critical blackstart requirement." For item 1.5, please provide a definition of "initial switching requirements" in the item language. For all other items in Attachment 1, PSEG concurs with and hereby incorporates by reference the comments filed by Edison Electric Institute ("EEI") in this matter.
Response: Thank you for your comments. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.5 – The term "initial switching requirements" came from EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started." This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."		
Pepco Holdings, Inc - Affiliates	Yes	PHI supports the comments of EEI for Attachment 1. In particular, we believe that the Planning Coordinator and Transmission Planner should be added to the applicability list. Also note that the terms "single plant

Organization	Yes or No	Question 2 Comment
		location" (1.1) and "single station location" (1.5) are undefined. EEI has also made clarifying language changes.
Response: Thank you for your comments. Since there is no Requirement that applies to the Planning Coordinator or the Transmission Planner, it is not appropriate to include them in the Applicability section. Please refer to the response to EEI's comments.		
MRO's NERC Standards Review Subcommittee	Yes	Item 1.4 Item 1.4 uniformly identifies all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans they provide to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable, as it provides well documented options should any problems occur. As currently written, Item 1.4 inadvertently provides incentive to utilities to remove resources from the restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, that would allow them to remain listed in the restoration plan without uniformly being identified as critical. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.15 and the capacity bright line of Item 1.13:"Each Blackstart Resource identified in the Transmission Operator's restoration plan as used to directly start generation identified as a Critical Asset, or identified in the Transmission Operator's restoration plan as used to directly start generation greater than an aggregate of 300 MW."We believe this approach should provide a better sense of a Blackstart Resource's true impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also addresses the inadvertent incentive for removing blackstart resources from the restoration plan. Item 1.7 We believe this bright line is overly simplistic, and does not provide an accurate measuring stick for defining critical Transmission Facilities. Per NERC TPL-001, we believe the Planning Coordinator or Transmission Planner already perform an annual near-term assessment that could be leveraged to provide a more accurate bright line. We would recommend rewording Item 1.7 as follows, leveraging the existing language of Item 1.7 and the capacity bright line of Item 1.1:"Each Transmission Facility operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher where the Planning Coordinator or Transmission Planner identifies the sum of the incoming power flows or the sum of the outgoing power flows to exceed 1500 MW."It would be our intention that this particular assessment be based on the forecasted

Organization	Yes or No	Question 2 Comment
		peak conditions using Category A of Table 1 of the TPL-001 standard. Item 1.13 We believe this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, we believe this item needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. This should only apply to firm load and not demand side management (DSM).Therefore, we believe this bright line should be reworded as follows:"A single common control system configured for performing automatic load shedding of 300 MW or more of firm load within 15 minutes." Item 1.14 We do not believe all control center/systems and backup control centers/systems performing the functional obligations of the Balancing Authority or Transmission Operator should uniformly be considered critical to the Bulk Electric System. We believe the previously proposed CIP-010 criteria 1.13 and 1.14 delineations based on MW or voltage levels should be maintained to provide a more accurate bright line for identifying critical systems. Items 1.8, 1.9, & 1.12 Criteria 1.8, 1.9, and 1.12 should be modified because loss of facilities does not cause an IROL violation. An IROL includes a limit and a time constant Tv. In order for an IROL violation to occur, the limit must be exceeded for at least the time constant Tv. Tv is usually 30 minutes. Thus, when we consider the impact on the loss of facilities on an IROL, an operator will have enough time to adjust the system to prevent an IROL violation. For 1.8, the criterion should be modified to reflect that the facilities that comprise an IROL should be considered critical. The drafting team may also wish to consider loss of any facilities that set up the need for the IROL as well or cause the actual limit to change. For criterion 1.9, it is not clear why FACTs devices need to be singled out. Are they not covered in criterion 1.8 under Transmission Facilities? Inclusion of 1.9 is redundant and just causes confusion because it causes the reader to infer that the drafting team intended for them to be treated differently when in fact the criterion is the same as 1.8. For criterion 1.12, it would be more appropriate to assess the impact of an SPS, RAS, or automated switching system on the IROL. If loss of the SPS, RAS, or automated switching system causes an IROL to decrease, then the SPS, RAS, or automated switching system should be considered critical. Contrary to the companion draft guidance document statement in the second paragraph on page 11, most SPS, RAS and automated switching systems are not used to prevent disturbances that would result in IROLs. In fact, some regions consider generation runback schemes to be an SPS even when it is used to simply resolve a generation outlet issue for loss of a line out of a plant. This is a common and economically effective way to avoid the expense of building more transmission lines. This paragraph from the draft guidance document should be

Organization	Yes or No	Question 2 Comment
		removed. Item 1.16 Recommend removal of this criterion, this criterion is arbitrary and doesn't constitute a bright line.
Response: Thank you for your comments. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. We will consider your suggested language in a future version when the topic of prioritization is addressed. Item 1.7 – The SDT does not feel that a power flow analysis would lead to a consistent application of the criterion, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – FACTS devices were singled out to ensure that there was no confusion as to whether or not they were considered Critical Assets. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
Santee Cooper	Yes	We believe the Attachment 1 criteria is too prescriptive and would add unnecessary economic and resource burdens. For example, we have made investments to ensure that redundant blackstart resources as well as redundant cranking paths are available where needed for restoration, and therefore any one blackstart

Organization	Yes or No	Question 2 Comment
		resource or cranking path is not critical to the viability of our restoration plans. Therefore, considering any one such blackstart resource or cranking path critical diminishes the value of our original investment in redundancy. We also believe the SDT's change in wording of criteria 1.13 may inappropriately apply to all SCADA systems with the capability of shedding load greater than 300 MW. Such a requirement should only apply to common control systems that are "configured" to perform automatic load shedding of 300 MW or more. We believe 1.16 in Attachment 1 should be deleted since it is not consistent with the "bright line" concept.
Response: Thank you for your comments Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
Dominion	Yes	Dominion has the following comments: 1.1 While we understand the SDT's reasoning for using net Real Power capability, we prefer the use of a more 'stable' value such as generator value (pMax, nameplate rating, etc.) used in the interconnection planning process. We have seen that the net Real Power capability fluctuates annually and have found that using such a value in compliance may not in the best interest of reliability. We began using the value cited in the interconnection planning process because it doesn't change often and any change is usually accompanied by change management process includes extensive communication between the Transmission Planner and Generator Owner. For this reason, we believe that this is a superior value to use. 1.15 Dominion believes the second criteria is overly conservative and is not necessary for reliability. We cite the following observations:(1) It is likely that many of the generators that will be designated critical assets will be nuclear (due to the typical large size of individual generators and the fact that there are usually more than one unit at each location). However, control and monitoring of nuclear generation is vastly different than other forms of generation (coal, oil, gas, and hydro). Nuclear units are typically either on-line (at very near rated

Organization	Yes or No	Question 2 Comment
		output) or are off-line. Therefore the 'control' of the units consists typically of outage coordination and reporting. The data used to monitor these units (typically mW and mVAr) may or may not be transmitted directly to the TOP. Where the data is transmitted directly to the TOP, the generation control center function consists primarily of outage coordination and reporting. This does not, in our view, warrant critical designation of the control center itself since this coordination and reporting can occur without such center.(2) Where other types of generators (peaking CTs, hydro, etc.) are operated in a manner similar to nuclear (on line at near rated output or off line), we view the control center function as being almost identical to that described above and therefore do not agree that such center should be designated as critical..(3) Where the generator output is not being controlled in a very dynamic manner (such as when proving ancillary services; regulation or spinning reserve), 'control' often consists of manual (verbal) dispatch to follow load (I.E. lower output during off-peak hours, higher during on-peak hours and near maximum during peak hours). It is not critical that such generator be dispatched from a designated location (control center), it could be done from almost anywhere that has the necessary communications infrastructure. Where this is true, we do not agree that the control center needs to be designated as critical. (4) We do not believe there is sound technical basis for the 1500 mw threshold. In ERCOT, this value represents approximately 1.4% of the total generation in that Interconnection. In the Western it represents 0.6% and in the Eastern, it represents .02%. We therefore suggest that this criterion be revised in a manner similar to one of the examples shown below: "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of; Example 1 - Based upon some ratio or multiple of frequency response for each Interconnection. This would involve more analysis but would set threshold based on the presumption that misuse could result in loss of all generators controlled by the generation control center and the impact of such loss could result in a drop in frequency of that interconnection to an 'unacceptable value' (perhaps that value is .02 Hz, .05 Hz, etc). Acceptance of this proposal might require such value be re-determined on a regular basis (annual, 5 year, ?) or based upon some trigger (large increase or decrease in total generation or frequency response within that interconnection). Example 2 - Set mw threshold based upon some percentage total generation in the interconnect, but insure that the resulting threshold is less than the sum of all load included in UFLS and UVLS programs within that Interconnect. For example, if UFLS and UVLS are based on 30% of system load, set this threshold at say 5-20% of total generation (verifying that the percentage chosen results in a threshold than is less than the sum of load shed programs.
Response: Thank you for your comments. Item 1.1 –The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest		

Organization	Yes or No	Question 2 Comment
value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line. Item 1.15 – A control center function includes Bulk Power System (BPS) and system status monitoring and processing for reliability and asset management purposes, such as providing information used by Responsible Entities to make operational decisions regarding the reliability and operability of the BPS. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Your proposal to use frequency response or percent of total load in an interconnection is similar to an approach taken by the SDT to use reserve sharing for the threshold for generation. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. The SDT believes that the same threshold should be used for generation control systems.		
Edison Mission Marketing and Trading	Yes	* Specify for who (function) the Requirements apply to as do other NERC Reliability Standards.* Replace the term 'Critical Assets' with 'Assets subject to Cyber Security Protection'.
Response: Thank you for your comments. The Applicability section of the standard specifies what NERC Registered Entities the standard applies to. All Requirements apply to all Entities listed in the Applicability section. Critical Asset is a defined NERC term and has been used for CIP Versions 1 to 3.		
Florida Municipal Power Agency	Yes	1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. FMPA Comments: FMPA commends the SDT for their attempted to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. However, FMPA continues to have the comment we submitted in CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. FMPA is concerned that the use of the “Real Power Capability of the preceding 12 months” would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2. SDT Proposed:1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. FMPA Comments: FMPA believes that this “bright line” is arbitrary and instead suggests combining this with 1.9. There is no significant difference between the MVARs provided by FACTs devices and those provided by a power plant and it makes sense to treat them both in the same fashion. SDT Proposed:1.3. Each generation Facility that the Planning Coordinator or Transmission Planner

Organization	Yes or No	Question 2 Comment
		designates as required for reliability purposes. FMPA Comments: FMPA commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. FMPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: "Adverse Reliability Impacts" will help clarify which units should be in this category. We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. FMPA proposes the following rewording of criteria 1.3:"1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer." SDT Proposed:1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. FMPA Comments: FMPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). FMPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective restoration plan, reducing the plan's overall robustness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, FMPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW. We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address

Organization	Yes or No	Question 2 Comment
		system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan. SDT Proposed:1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. FMPA Comments: FMPA commends the SDT on differentiating between a single Cranking Path as a critical facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. FMPA suggests that the SDT change "switching requirements" to "switching equipment." SDT Proposed:1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. FMPA Comments: FMPA believes that criteria 1.7 is rather arbitrary and suggests use of TPL-004-0 Category D testing and to combine 1.7 with 1.8. Does loss of a substation result in an IROL or Adverse Reliability Impacts? Doing so can also remove the voltage class limit. It is also unclear from the working whether the entire substation is a Critical Asset, or whether each Facility connected to that substation is a Critical Asset. FMPA suggests the entire substation. It is also unclear for substations that have two voltage levels (e.g., a 345 kV to 115 kV substation), whether the entire substation should be considered, or just one voltage level. FMPA suggests one voltage level as discussed in the existing TPL-004 standard. SDT Proposed:1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse Reliability Impact would be beneficial. Proposed rewording of criteria 1.8:1.8. Transmission Facilities at a single station or substation that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs) or can cause an Adverse Reliability Impact as a result of extreme contingency loss of substation testing as part of the TPL standards or as determined by the Reliability Coordinator. SDT Proposed:1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that criteria 1.9 should be reworded to "station or substation" instead of just

Organization	Yes or No	Question 2 Comment
		"station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse Reliability Impact would be beneficial. SDT Proposed:1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that adding the phrase “or can cause an Adverse Reliability Impact” would be beneficial. SDT Proposed:1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. FMPA Comments: FMPA believes that the 300 MW is arbitrary and seems based more on reporting requirements than on true reliability impacts. Also, it should not matter whether loss of load is caused by an “automatic” system or not. In addition, the power system is more resilient to loss of load than loss of generation; hence, by using the same threshold as is used in 1.1, we are actually being quite conservative. FMPA offers the following alternatives for rewording 1.13:1.13 Common control system(s) that can result in a loss of load equal to or greater than the reserve sharing requirements of the Reserve Sharing Group within 15 minutes. SDT Proposed:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. FMPA Comments: FMPA is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15.FMPA offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system that can:1.14.1 Cause a loss of generation or load greater than the reserve sharing requirements of the Reserve Sharing Group1.14.2 That if manipulated, can cause an Adverse Reliability Impact as determined through planning studies. FMPA cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability, cascading or uncontrolled separation of the BES. SDT Proposed:1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. FMPA Comments: With the proposed revision to 1.14, this 1.15 would no longer be required.

Organization	Yes or No	Question 2 Comment
		SDT Proposed:1.16. Any additional assets that the Responsible Entity deems appropriate to include. FMPA Comments: FMPA believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Response: Thank you for your comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. In addition, the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method.

Item 1.2 – The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality. FACTS devices in 1.9 are specifically related to IROLs, whereas the reactive resources in 1.2 are not limited to IROL applications.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.7 –The SDT does not believe that power flow based bright-line criteria (i.e. using TPL-004-0) would meet the objective of uniform application of Critical Asset identification across all entities. The term Transmission Facilities can be applied to either the entire substation or each Facility or group of Facilities connected to that substation, as determined by the entity. This would allow an entity which has multiple voltage levels at a single substation to either declare the

Organization	Yes or No	Question 2 Comment
		entire substation as a Critical Asset or only the portion of the substation that qualifies under criterion 1.7. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 –The SDT agrees to change "stations" to "stations or substations." The SDT does not believe that power flow based bright-line criteria (i.e. using TPL standards) would meet the objective of uniform application of Critical Asset identification across all entities. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 - The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.12 – By limiting the scope of Criterion 1.12 to IROLs, Adverse Reliability Impacts are covered as well. This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 – This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.
PNGC Power	Yes	We associate ourselves with NRECA comments: 1. We're concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). We understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities

Organization	Yes or No	Question 2 Comment
		include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a Critical Asset. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, we would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. 2. In item 1.7 the statement regarding "three or more other transmission stations" is confusing. A better explanation is needed -- does this mean stations upstream, downstream, networked or radial? 3. In item 1.14 the term "control center" must be defined, especially when dealing with the significance of the requirements of this standard. Using an undefined term here is inappropriate. 4. In item 1.14 its states that all RC, BA and TOP control centers, etc., are Critical Assets. While NRECA agrees with this as it relates to RCs, we do not agree with this as it relates to all BAs and TOPs. In the draft CIP-010 there was high, medium and low criteria which in many instances appropriately matching CIP requirements to the level of risk certain assets potentially present to the BPS. NRECA strongly believes that the CIP-002-4 standard requirements for smaller BAs and TOPs should match the lower level of risk to BPS reliability that these smaller BAs and TOPs potentially present. Similar to the 1500MW size criteria that is included in item 1.15 for generator control centers, there should be size criteria for the smaller BAs and TOPs. The drafting team should modify item 1.14 to state that all control centers with a peak demand above 2000MW (same as medium criteria in draft CIP-010) shall be designated as a Critical Asset. This is the lowest NRECA could support and also recommend its members to support. We firmly believe that this would capture all of the control centers that truly have a material impact on the reliability of the BPS. 5. Related to the Critical Asset Criteria, there should be a provision in the standard that provides a process for an entity to technically demonstrate that even though the criteria identifies some of their assets as Critical Assets, their assets (or a portion thereof) do not meet the definition of a Critical Asset and should be excluded from applicability of CIP-003 through CIP-009.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. Item 1.7 – The intent of criterion 1.7 is to classify as a Critical Asset Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.14 - At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.		
WECC		No specific recommended changes, but some stakeholders have indicated the criteria will lead to the identification of FEWER Critical Assets. Please reveiw for appropriateness.
Response: Thank you for your comments.		
Southern Company	Yes	Southern recommends the following changes: 1.6. Transmission Facilities operated at 500 kV or higher Voltage alone is not a sufficient criterion to determine whether or not an asset is critical to the bulk electric system. Southern believes that the way the asset is interconnected should also be included as a portion of the criteria. Accordingly, Southern suggests the SDT delete Section 1.6 based on the comments stated in this paragraph and the protections offered

Organization	Yes or No	Question 2 Comment
		under Section 1.7. Southern agrees with the SDT's proposed language for criterion 1.11 and believes it is important for this criterion to continue to incorporate the language from NUC-001-2 (i.e., "identified as essential to meeting Nuclear Plant Interface Requirements"). To make Section 1.14 consistent with the language in Section 1.15, Southern recommends the following changes to Section 1.14: 1.14. Each control center and , backup control center used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Southern recommends the following change to Section 1.16: 1.16. Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include.
Response: Thank you for your comments. Item 1.6 – The drafting team believes all Transmission Facilities operated at 500 kV or higher do not require any further qualification for their role as components of the backbone on the interconnected BES. Item 1.11 – Thank you for your comment. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
Encari, LLC	No	
Arizona Public Service	No	
Edison Electric Institute	Yes	EEI offers the following suggestions for Attachment 1: 1.1 EEI Comment: The phrase "single plant location" is undefined. It is unclear if this means at a single street address or within some number of miles. 1.3 Substitute Text: Each generation Facility that the Planning Coordinator or Transmission Planner has

Organization	Yes or No	Question 2 Comment
		designated as required to avoid one or more reliability criteria violations. 1.3 EEI Comment: The purpose of these changes is to facilitate the Planning Coordinator or Transmission Planner the opportunity to identify Generation Facilities that have been historically required to support the BES. This criteria is not meant to create the need for new or different planning models to be used by the Planning Coordinator or Transmission Planner. 1.5 Substitute Text: The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where two or more path options exist. 1.8 Substitute Text: Transmission Facilities at a single station location that the Planning Coordinator or Transmission Planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations. 1.8 EEI Comment: The phrase “single station location” is undefined. It is unclear if this means at a single street address or within some number of miles. The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency facilities communicated by the PC and TP per requirement R5 of FAC-014. This criteria is not meant to create the need for new or different planning models to be used by the Planning Coordinator or Transmission Planner. Rather, they should continue to use the legacy planning models as specified in FAC-010, FAC-011 and FAC-014. 1.9 Substitute Text: Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROLs) violations. 1.11 Substitute Text: Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements. 1.12 Substitute Text: Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROLs) violations for failure to operate as designed. 1.14 Substitute Text: Each control center, or backup control center, used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. 1.14 EEI Comment: Made consistent with 1.15 1.16 Substitute Text: Any additional assets owned by the Responsible Entity that the Responsible Entity

Organization	Yes or No	Question 2 Comment
		deems appropriate to include.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.

Tennessee Valley Authority	Yes	1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. The language

Organization	Yes or No	Question 2 Comment
(TVA)		appears to require us to designate "Each" component in the System Restoration plan as CA. Because we currently have black start procedures which include at least 2 paths for black start of most generation plants in the system, the proposed language would require the extension of CA designation to a large number of components which otherwise would not be included by other criteria. The flexibility provided by our robust transmission infrastructure and the large number of black start capable plants serves to ensure reliable operation of the BES, but designating as a CA each component that could participate in the total paths possible doesn't seem consistent with the intent of the standard. Recommendation: Revise language to allow entities to limit CA designation to those components participating in the primary black start path. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.There isn't a clear definition of the term "directly connected." Without this definition there are many way to interpret this requirement. Is this language meant to describe a facility where the substation is co-located with a generation facility? Also, does the language this mean total loss of substation or only partial? Recommendation: For the purpose of this standard revise language to clearly define "directly connected."
Response: Thank you for your comments. Item 1.4 – The SDT used the word "primary" in its initial posting of CIP-010-1, but received industry feedback that the term was confusing and it is not a defined NERC Glossary term, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any transmission Facility the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include the partial or total loss of a substation. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."		
PacifiCorp	Yes	: PacifiCorp suggests improvements to several of the current Critical Asset criteria in Attachment 1: Criteria 1.8, 1.9, and 1.12 currently refer to certain assets that could violate one or more Interconnection

Organization	Yes or No	Question 2 Comment
		Reliability Operating Limits (IROLs). However, the term "IROL" is not generally utilized within the Western Electricity Coordinating Council (WECC). Instead, WECC uses the term System Operating Limits (SOLs). The Standards Drafting Team should supplement these criteria to reflect this distinction. PacifiCorp suggests the following language: "...violate one or more Interconnection Reliability Operating Limits (IROLs), or, for WECC members, System Operating Limits (SOLs) for the transfer paths identified in the most current list of Major WECC Transfer Paths in the Bulk Electric System." Criterion 1.9 currently refers to "Flexible AC Transmission Systems (FACTS) at a single station location," but NERC offers no uniform definition for this term. Such a scenario could lead to confusion among responsible entities, as many devices could be considered FACTS, including static VAR compensators (SVC), D-VAR (Dynamic VAR), synchronous condensers, series caps, STATCOM, and phase shifters. As such, a definition for FACTS should either be included in Attachment 1 or added to the NERC Glossary of Terms.
Response: Thank you for your comments. Items 1.8, 1.9, and 1.12 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. Criterion 1.8 has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.9 has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.12 has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.9 - FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Commonly accepted terms and definitions do not require an insertion in the NERC Glossary.		
OGE	Yes	(In General) Clarify Attachment 1 criteria to minimize the interpretation variance. (1.1) Add more specificity to the term "location".(1.1) Refer to MOD-024 within the standard. For the 1500 MW "bright line"; it needs to be perfectly clear which units are included. (1.3) This criteria is open for auditors to interpret; standards should not be this open-ended. Use language that requires that the facilities be formally designated as "required for reliability purposes", in advance. (1.4) Change to "Each resource designated as a Blackstart Resource in the Transmission Operator's restoration plan as required in EOP-005." If a resource is "also mentioned" and/or is "Blackstart capable", it is not necessarily a Critical Asset. (1.5) This criteria conflicts with the NERC Glossary definition for the term "Cranking Path". The glossary does

Organization	Yes or No	Question 2 Comment
		not specify multiple path options, yet the criteria indicates "up to the point on the Cranking Path where multiple path options exist". By NERC definition, the cranking path may connect two generation resources and never have multiple options. Include in the criteria "Where multiple path options do not exist, the entire Cranking Path is included."(1.5) Should this criteria include a time element? Must this be a permanent "Cranking Path"? (1.6) The criteria compounds the NERC Glossary terms "Transmission" and "Facilities" which is inappropriate. A new "local" definition for the term "Transmission Facilities" should be derived for use in this standard and proposed as an addition to the NERC glossary.(1.6) The criteria appears to include transmission lines as Critical Assets. The overhead associated with tracking all 500+ kV transmission line segments, breakers, busses, and other equipment is excessive.(1.6) Consider using capacity instead of nominal voltage level as the bright line. Dual 345kV lines may be used in place of a single 765kV line. Although there may be independent cyber assets, the loss of either will have a similar impact to the BES. (1.7) The criteria compounds the NERC Glossary terms "Transmission" and "Facilities" which is inappropriate. A new "local" definition for the term "Transmission Facilities" should be derived for use in this standard and proposed as an addition to the NERC glossary.(1.7) Locally define and explicitly exclude "Generation Interconnection Facilities" from this criteria. This term is used in the NERC document, "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface" located at http://www.nerc.com/files/GO-TO_Final_Report_Complete_2009Nov16.pdf. (1.10) See [1.7] comment "Locally define..." (1.13) Define "automatic" within the standard.(1.13) Use the same "bright line" as generation, 1500 MW. While understood it is a reporting threshold, it is difficult to understand how the loss of 300 MW has a significant impact to the reliable operation of the BES. (1.15) Distinguish between Control Center and Control Room within the Standard or attachment.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant. It is NERC's practice not to directly refer to other standards by name in developing standard language.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the

Organization	Yes or No	Question 2 Comment
System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." Based on the glossary term Blackstart Resource, the SDT has determined that the reference to EOP-005 is unnecessary. It is NERC's practice not to directly refer to other standards by name in developing standard language. Item 1.5 – Cranking Path is defined as "A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units." It does not specify multiple paths, but it also does not exclude them. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.6 – The SDT appropriately uses the phrase "Transmission Facilities." The SDT is referring to Facilities that comprise Transmission. The issue with using capacity (or rating) instead of voltage level does not meet the objective of uniform application of Critical Asset identification across all entities. Item 1.7 – The SDT appropriately uses the phrase "Transmission Facilities." The SDT is referring to Facilities that comprise Transmission. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to a radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.10 – The SDT appropriately uses the phrase "Transmission Facilities." The SDT is referring to Facilities that comprise Transmission. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.15 – Control centers generally perform control functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control functions for a single BES asset should be evaluated as part of BES asset (e.g., control room for a single generation plant or transmission substation).		
FMPA	Yes	1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. FMPA Comments: FMPA commends the SDT for their attempted to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. However, FMPA continues to have the comment we submitted in CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. FMPA is concerned that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to

Organization	Yes or No	Question 2 Comment
		certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2. SDT Proposed:1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. FMPA Comments: FMPA believes that this “bright line” is arbitrary and instead suggests combining this with 1.9. There is no significant difference between the MVARs provided by FACTs devices and those provided by a power plant and it makes sense to treat them both in the same fashion. SDT Proposed:1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes. FMPA Comments: FMPA commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. FMPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: “Adverse Reliability Impacts” will help clarify which units should be in this category.We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. FMPA proposes the following rewording of criteria 1.3:”1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer.” SDT Proposed:1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. FMPA Comments: FMPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). FMPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator’s restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective restoration plan, reducing the plan’s overall robustness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource’s actual

Organization	Yes or No	Question 2 Comment
		role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, FMPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW.We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan. SDT Proposed:1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. FMPA Comments: FMPA commends the SDT on differentiating between a single Cranking Path as a critical facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. FMPA suggests that the SDT change "switching requirements" to "switching equipment." SDT Proposed:1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. FMPA Comments: FMPA believes that criteria 1.7 is rather arbitrary and suggests use of TPL-004-0 Category D testing and to combine 1.7 with 1.8. Does loss of a substation result in an IROL or Adverse Reliability Impacts? Doing so can also remove the voltage class limit. It is also unclear from the working whether the entire substation is a Critical Asset, or whether each Facility connected to that substation is a Critical Asset. FMPA suggests the entire substation. It is also unclear for substations that have two voltage levels (e.g., a 345 kV to 115 kV substation), whether the entire substation should be considered, or just one voltage level. FMPA suggests one voltage level as discussed in the existing TPL-004 standard. SDT Proposed:1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse

Organization	Yes or No	Question 2 Comment
		Reliability Impact would be beneficial. Proposed rewording of criteria 1.8:1.8. Transmission Facilities at a single station or substation that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs) or can cause an Adverse Reliability Impact as a result of extreme contingency loss of substation testing as part of the TPL standards or as determined by the Reliability Coordinator. SDT Proposed:1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse Reliability Impact would be beneficial. SDT Proposed:1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). FMPA Comments: FMPA believes that adding the phrase “or can cause an Adverse Reliability Impact” would be beneficial. SDT Proposed:1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. FMPA Comments: FMPA believes that the 300 MW is arbitrary and seems based more on reporting requirements than on true reliability impacts. Also, it should not matter whether loss of load is caused by an “automatic” system or not. In addition, the power system is more resilient to loss of load than loss of generation; hence, by using the same threshold as is used in 1.1, we are actually being quite conservative. FMPA offers the following alternatives for rewording 1.13:1.13 Common control system(s) that can result in a loss of load equal to or greater than the reserve sharing requirements of the Reserve Sharing Group within 15 minutes. SDT Proposed:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. FMPA Comments: FMPA is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15.FMPA offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system that

Organization	Yes or No	Question 2 Comment
		can:1.14.1 Cause a loss of generation or load greater than the reserve sharing requirements of the Reserve Sharing Group1.14.2 That if manipulated, can cause an Adverse Reliability Impact as determined through planning studies. FMPA cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability, cascading or uncontrolled separation of the BES. SDT Proposed:1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. FMPA Comments: With the proposed revision to 1.14, this 1.15 would no longer be required. SDT Proposed:1.16. Any additional assets that the Responsible Entity deems appropriate to include. FMPA Comments: FMPA believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.
Response: Thank you for your response. Please refer to the response to comments of Florida Municipal Power Agency.		
South Carolina Electric and Gas	No	
Pinellas County Resource Recovery Facility	No	
Central Lincoln	Yes	The standard needs a definition of “Control Center.” The guidance document contains one, but is not part of the standard. And the one in the guidance document could be interpreted to apply to any laptop or PDA that could be used to control more than one BES asset. Suggest that “Control Center” be defined to be a fixed location.
Response: Thank you for your comments. At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect.		
Edison Mission Marketing and Trading	Yes	CIP-002-4 Attachment 1-1.1 what is the basis for the 1500 MW versus what used to be Output exceeds Reserve Sharing Group obligation or Output exceeds Contingency Reserve obligation?

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.		
SPS Consulting Group Inc.	Yes	Criteria 1.3 states: "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." The term "designates" should be deleted and replaced with "demonstrates through independently verified engineering assessments". The problem with the current ability to simply designate a generator as a critical asset is that not all Planning Coordinators and Transmission Planners are independent. There is a significant competitive incentive for the non-independent PCs and TPs to label a competitor as "critical", thereby increasing their cost of operation and decreasing their competitiveness. No entity should be able to simply "designate" another as having critical assets.
Response: Thank you for your comments. Item 1.3 – The burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. This criterion has been reworded to “Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.” If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, then that unit must be classified as a Critical Asset. If an entity feels that they have an asset that has been unjustly classified as “required for reliability reasons,” there are NERC appeals processes that can be used. The Planning Authority and/or Transmission Planner are not designating the asset as critical for CIP purposes; they are determining the unit to be necessary to avoid Adverse Reliability Impacts based on other NERC reliability standards.		
Tacoma Power	Yes	Comments: For Section 1.1, Tacoma Power commends the SDT’s attempt to set a bright line for generating units based on a significant operational threshold. However, the bright line criterion of 1500 MW for all regions is not realistic. The bright line criterion should be determined based on the requirements of each region. Tacoma Power also agrees with APPA’s suggestion of using the FAC-009-1 R2 facility ratings. Therefore, Tacoma Power suggests Section 1.1 be changed to read, “Each group of generating units (including nuclear generation) at a single plant location with an aggregate FAC-009-1 facility rating equal to or exceeding the MW value set by the Regional Reliability Organization.” For section 1.2, Tacoma Power agrees with the need to set a bright line limit but suggests that the bright line limit again be set by the Regional Reliability Organization based on the regional system. Therefore, Tacoma Power suggests the following language, “Each reactive resource or group of resources at a single location (excluding Generation Facilities) having an aggregate net Reactive Power nameplate rating at or above the

Organization	Yes or No	Question 2 Comment
		value set by the Regional Reliability Organization." For section 1.3, Tacoma Power commends the SDT for adding a criterion for including generation facilities that do not fall under the section1.1 criterion. However, Tacoma recommends the language be changed to read, "Any generation Facility that the Planning Coordinator or Transmission Planner designates, provides justification for and receives concurrence from the RRO as required for reliability." For Section 1.4, Tacoma Power has no comments. For Section 1.5, Tacoma Power has no comments. For Section 1.6, Tacoma Power has no comments. For Section 1.7, Tacoma Power has no comments. For Section 1.8, Tacoma Power has no comments. For Section 1.9, Tacoma Power has no comments. For Section 1.10, Tacoma Power has no comments. For Section 1.11, Tacoma Power has no comments. For Section 1.12, Tacoma Power has no comments. For Section 1.13, Tacoma Power concurs with APPA's comments when they said, "APPA believes the SDT's change in wording of criteria 1.13 will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. As written, this criteria designates as a critical asset various control systems that by themselves could not cause instability or uncontrolled separation of the BES.APPA offers the following alternatives for rewording 1.13:1.13 Common control system(s) configured to perform automatic load shedding of 300 MW or more within 15 minutes. APPA can accept the bright-line of 300 MW if the wording is changed to that stated above, but we still see this bright-line as an arbitrary threshold based on a quantity that has no BES operational significance. Rather, 300 MW is a DOE threshold for electric event reporting." For section 1.14, Tacoma power concurs with APPA's comments when they say:"APPA is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria [sic] to include a bright-line with similar impact as those in 1.1 and 1.15.APPA offers the following revised wording: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. APPA cannot support this standard revision without some form of bright line cutoff

Organization	Yes or No	Question 2 Comment
		to exclude small BAs and TOPs that cannot cause instability or uncontrolled separation of the BES. However, we will support inclusion of "ALL BA and TOP control centers" only when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal." For Section 1.15, Tacoma Power has no comments. For Section 1.16, Tacoma Power has no comments.
Response: Thank you for your comments. Item 1.1 - The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. Item 1.2 – The issue with using different MVAR values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
Green Country Energy	No	
Illinois Municipal Electric Agency	Yes	IMEA recommends that Criterion 1.8 be continued with the following language: "...(IROLs) as demonstrated by the Reliability Coordinator." If the RC is not appropriate, it may be necessary to add the appropriate functional enttity, for demonstrating IROLs, to Applicability section 4.1. This additional language will clarify that the TO, LSE, etc. is not responsible for demonstrating IROLs.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.8 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."		
Minnkota Power Cooperative	Yes	1.12: MPC agrees with criteria 1.12, however the guidance document states that "Since the purpose of SPS and RAS is to prevent disturbances that would result in excursions beyond IROLs.... it is expected that all such systems and schemes will be designated as Critical Assets." MPC disagrees with the statement that this is the purpose of all SPS and RAS.
Response: Thank you for your comments. Please refer to the updated guidance document.		
Horizon Wind Energy	Yes	Criteria 1.15 in attachments A includes generation control centers used to control generation greater than an aggregate of 1500 MWs in a single interconnection. It is true that the span of control of the generation control center may cross multiple BA or RSG areas. In the unlikely event of a common mode failure of such a generation control center that would lead to a loss of all generation, the loss of generation in the multiple BAs or RSGs could fall significantly below the criteria of the 1500 MWs threshold used in criteria 1.1 for generating units at a single plant location, therefore not affecting the reliability and operability of the BES system. There seems to be a disconnect in criteria 1.1 for generation and 1.15 for generation control centers, hence 1500 MWs in a single plant location vs. 1500 MWs aggregate in a single interconnection for generation control centers. Secondly, some generation control centers collect data from generators via SCADA for monitoring purposes and can manually send set points to lower generation if the need would arise. Does this type of arrangement fall under the description of control generation or was it the intent to include, in the description, generation that is controlled to maintain sufficient Contingency Reserve (BAL - 002) and Resource and Demand Balancing (BAL - 003)? Suggest adding language to 1.15 that is more in line with the criteria in 1.1 and clarifying what is meant by control generation.
Response: Thank you for your comments. Item 1.15 – Thank you for your comment. This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Generation control centers that collect data from generators via SCADA for monitoring purposes and have the ability to manually send set points to lower generation if the need would arise and meet the specifications of criterion 1.15 would be considered Critical Assets. For further information, please refer to the updated guidance document.		

Organization	Yes or No	Question 2 Comment
Union Power Partners LP	Yes	I suggest the inclusion of the "common mode" concept, for without a CM system, an outside intruder absolutely cannot obtain control of the entire generating capability at one time. I also, believe there should be some type of exceptions for small companies that do not have the financial capacity to implement all requirements. Are there some requirements that are more important than others which could provide a "floor" of physical & cyber security?
Response: Thank you for your comments. The "common mode" concept is reflected in the identification of Critical Cyber Assets in Requirement R2. Once an asset is identified as a Critical Cyber Asset, it must be compliant with all of the requirements in CIP-003 to CIP-009.		
MidAmerican Energy Company	Yes	MidAmerican Energy Company would like to provide the following suggestion for Critical Asset criteria 1.9 in Attachment 1:Criterion 1.9 does not define "Flexible AC Transmission Systems (FACTS)." A definition for FACTS should either be included in Attachment 1 or added to the NERC Glossary of Terms.
Response: Thank you for your comments. Item 1.9 – FACTS is defined by IEEE as: "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Commonly accepted terms and definitions do not require an insertion in the NERC Glossary.		
North Carolina Membership Corporation	Yes	NCEMC agrees with the following NRECA Comments: 1. What is the technical justification for the proposed criteria? The "Rationale and Implementation Reference Document" does not provide technical justification, but rather provides more of an opinion of the drafting team. To the extent possible, there should be technical justification for the proposed criteria that stakeholders can review. 2. In item 1.7 the statement regarding "three or more other transmission stations" is confusing. A better explanation is needed -- does this mean stations upstream, downstream, networked or radial? 3. In item 1.14 the term "control center" must be defined, especially when dealing with the significance of the requirements of this standard. Using an undefined term here is inappropriate. 5. Related to the Critical Asset Criteria, there should be a provision in the standard that provides a process for an entity to technically demonstrate that even though the criteria identifies some of their assets as Critical Assets, their assets (or a portion thereof) do not meet the definition of a Critical Asset and should be excluded from applicability of CIP-003 through CIP-009.
Response: Thank you for your comments.		

Organization	Yes or No	Question 2 Comment
The SDT believes information provided in the guidance document (posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf) provides sufficient technical justification for each criterion. Item 1.7 - The intent of Item 1.7 is to classify as a Critical Asset any Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.14 - At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. The SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.		
Hydro One Networks Inc.	No	2. We do not agree with criteria 1.6 and 1.7 in Attachment 1 as written. Application of these criteria would result in the inclusion of facilities that will have no impact on the BES reliability. We believe that the list of applicable facilities should be determined following an impact-based assessment to be performed by the Reliability Coordinator. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct/review the assessment should be included. We therefore propose the following wording to replace 1.6 and 1.7 in Attachment 1: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.1.7 Transmission Facilities operated at 300 kV or higher to less than 500 kV at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages.
Response: Thank you for your comments. Items 1.6 and 1.7 – The SDT does not feel that a power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."		

Organization	Yes or No	Question 2 Comment
Dynegy Inc.	Yes	For 1.1 and 1.15, why is 1500 MW the new value? Each draft document that comes out has had different criteria/values. How does the recent survey fit into this? I realize the Rationale and Implementation Reference Document mentions the Contingency Reserve concept mentioned in previous drafts but it does not seem right that one size (i.e. 1500 MW) should fit all Regions. Suggest a better fit by Region. For 1.3, the Rationale and Implementation Guidance Document uses the term "local area" to help determine if a unit is designated as this type of Critical Asset but it is unclear what "local" means. Please provide additional guidance. For 1.15, the draft Standard and Rationale and Implementation Guidance Document uses the term "control generation" to help determine if a unit is designated as this type of Critical Asset but it is unclear what "control generation" means. Please provide additional guidance.
Response: Thank you for your comments. Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Item 1.3 –This criterion has been reworded to “Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.” Item 1.15 –This criterion has been changed to “Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection.”		
Matrikon Inc.	Yes	The approval of CIP-002-4 is expected to bring in more Critical Assets that are subject to NERC CIP compliance. With this will be organizations that have never experienced CIP and will have a steep learning curve ahead of them. Guidance documents such as the one created unofficially by the SDT for CIP-002-4, as well as compilation of Q&A from Technical Webinars similar to the original FAQ attached to CIP version 1 is highly recommended. There is going to be many organizations looking to clarify how their assets are classified as per Attachment 1, and examples will be helpful.
Response: Thank you for your comments. The SDT is continuing to develop and refine the documents mentioned in your comments.		
Northeast Utilities	Yes	CIP-002-1 Attachment 1 criterion 1.3 reads: “Each generation facility that the planning coordinator or transmission planner designates as required for reliability purposes”. We believe that as stated, this criterion (1.3) is subject to interpretation. Specifically, “for reliability purposes” can be interpreted as “must-run” units,

Organization	Yes or No	Question 2 Comment
		required for black start (although that could be duplicative to criteria 1.4), or as any generator containing BPS elements. Suggest more clearly defining "for reliability purposes" or restating the criterion. The terminology used in the recent NERC data request appeared to be clearer - that is: "Any generation facility that the planning coordinator identifies as Reliability 'must run' assigned units". CIP-002-1 Attachment 1 criterion 1.10 reads: "Transmission facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3." We believe that as stated, this criterion (1.10) could be interpreted to mean not only generators owned by the responsible entity but also those not owned by but interconnected to the Transmission Owner's system. Clarification of criterion 1.3 should serve to clarify criterion 1.10 as well.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.10 – The SDT agrees that not only generators owned by the Responsible Entity but also those not owned by but interconnected to the Transmission Owner's system are subject to criterion 1.10. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."		
CenterPoint Energy	Yes	CenterPoint Energy believes the proposed criteria contained in Attachment 1 are generally reasonable. CenterPoint Energy is concerned that designation of assets under criteria 1.3 relies upon a risk-based assessment in the same manner that designation under the existing requirements of CIP-002-3 relies upon a risk-based assessment. Stated otherwise, criteria 1.3 does not appear to be a true "bright line" criteria. CenterPoint Energy is also concerned that requirements 1.8, 1.9, and 1.12 may create confusion among industry practitioners and inconsistent application by reliability auditors. Notwithstanding these concerns, CenterPoint Energy can support the requirements provided in Attachment 1 except criteria 1.11. As CenterPoint Energy understands it, the SDT believes criteria 1.11 is a "bright line" because NUC-001-2 Requirement 9.2.2 requires identification of facilities needed to meet the Nuclear Plant Interface Requirements (NPIRs). Therefore, Transmission Facilities designated as being essential to meeting NPIRs under NUC-001-2 Requirement 9.2.2 would be designated as Critical Assets under CIP-002-4.However, like proposed criteria 1.3, this criteria is not a true "bright line" because it requires a negotiated risk-based assessment to determine NPIRs pursuant to NUC-001-2 Requirement 2 and then to determine the facilities essential to meeting the NPIRs pursuant to NUC-001-2 Requirement 9.2.2. Therefore, it suffers the same flaw as the alleged flaw in CIP-002-3 and the previously noted flaw reflected in criteria 1.3 in

Organization	Yes or No	Question 2 Comment
		Attachment 1 of CIP-002-4. Additionally, unlike criteria 1.3, criteria 1.11 is not based upon BES reliability considerations. As indicated in the Purpose section of NUC-001-2, the requirements contained in NUC-001-2 are based upon ensuring safe operation and shutdown of nuclear plants. However, as indicated in the Purpose section of CIP-002-4, the "bright line" criteria contained in Attachment 1 is supposed to be criteria related to BES reliability, not criteria related to the safe operation and shutdown of nuclear plants. Therefore, it is misleading and inappropriate to include criteria 1.11 in Attachment 1. CenterPoint Energy is not suggesting that physical and cyber security of facilities required to ensure safe operation and shutdown of nuclear plants is not important. Physical and cyber security of such facilities is an important consideration and is already addressed under NUC-001-2 Requirement 9.3.6.In the context of CIP-002-4, where critical assets are determined based on BES reliability considerations, CenterPoint Energy is concerned that the inclusion of criteria 1.11 will create unnecessary confusion. One point of confusion is that facilities essential to meeting NPIRs under NUC-001-2 R9.2.2 are not necessarily limited to transmission facilities as indicated in CIP-002-4 Attachment 1, criteria 1.11. For example, a NPIR might be that voltage at a substation interconnecting nuclear plants needs to be maintained in a specified range under certain operating conditions. Since voltage control is provided by generators (by regulating reactive power output) in coordination with operation of transmission facilities, it is possible that one or more generating units (particularly the nuclear generating units and nearby generating units) might be designated as facilities essential to meeting the NPIR. The same is true for NPIRs relating to maintaining short circuit current below a specified level. If criteria 1.11 had merit, there is no logical reason why generating facilities potentially identified pursuant to NUC-001-2 R9.2.2 as being essential to meeting NPIRs would not be identified as Critical Assets yet under criteria 1.11 only transmission facilities would be so designated.The point is that proposed criteria 1.11 is an unnecessary criteria that inappropriately and incorrectly mixes the BES reliability considerations in CIP-002-4 with the nuclear plant safety considerations addressed in NUC-001-2. CenterPoint Energy is concerned that the confusion resulting from this inappropriate and incorrect blend of CIP and NUC related matters runs afoul of the stated goal of CIP-002 version 4 to create a clear, unconfusing "bright line" criteria. As a practical matter, besides physical and cyber security of NPIR-related assets being addressed by NUC-001-2 R9.3.6, the nuclear plant and associated switchyard would likely be designated as Critical Assets under CIP-002-4 Attachment 1 criteria 1.1 and 1.10 and possibly under one or more of the other criteria contained in Attachment 1. In summary, criteria 1.11 is an unnecessary, inexact, and confusing attempt to duplicate the concepts found in NUC-001-2 R9.2.2 and R9.3.6. As such, criteria 1.11 should be deleted in its entirety. Alternatively, if the SDT feels compelled to maintain proposed criteria 1.11 in Attachment 1, CenterPoint Energy proposes re-wording criteria 1.11 along the lines of proposed criteria 1.10, such as "Transmission Facilities providing the generation connection required to directly connect nuclear plant generator output to the transmission system." Although this alternative would still inappropriately mix the nuclear plant safety considerations found in NUC-001-2 with the BES reliability considerations that are the alleged basis for Critical Asset determination in CIP-002-4, this alternative would at least provide a "bright line" criteria. CenterPoint Energy could support either of these alternatives, but cannot support criteria 1.11 as it is currently

Organization	Yes or No	Question 2 Comment
		written.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Items 1.8, 1.9, and 1.12 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. Criterion 1.8 has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.9 has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.12 has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.11 – Designating facilities already determined necessary for another standard (i.e. NUC-001-2) does not constitute a risk-based approach to the identification of Critical Assets. Once those facilities have been identified, a bright line exists for inclusion as a Critical Asset. This is similar to the approach taken for IROLs.		
LCEC	Yes	Attachment 1: Paragraph 1.14 includes the Transmission Operator (TOP) function in addition to the Reliability Coordinator (RC) and Balancing Authority (BA) functions. In CIP10 the concept of a true "risk based" approach to the application of security requirements was proposed in the purpose section of the document as follows: Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES. The concept of matching security controls with risk is common practice that is found in NIST and ISO guidelines for risk management. These best practices should be leveraged when considering the implementation of CIPv4 and the development of future standards such as CIP10 and CIP11 that will include requirements for medium and low risk BES Cyber Systems. In the draft release of CIP10, the Balancing Authority (BA), Reliability Coordinator (RC) and Transmission Operator (TOP) functions were listed separately and with additional qualifying criteria. This is a much better approach that is well aligned with best practices and future standard development. When considering the proposed CIPv4 criteria, the control centers for the Transmission Operator (TOP) function should only be included as Critical Assets if they operate transmission facilities that meet the critical asset bright line criteria listed in paragraph 1.6 (above 500kV) or 1.7 (300Kv or

Organization	Yes or No	Question 2 Comment
		higher at stations interconnected at 300kV or higher with three or more other transmission stations). Not including these criteria will result in Non-Critical Assets being identified as Critical Assets. In addition, the standards will go against established best practices and be in conflict with the already released draft of the CIP10 and CIP11 standards. Suggested change to Attachment 1 paragraph 1.14:Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator or Balancing Authority. Suggested change to Attachment 1 (Add paragraph 1.x):Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Transmission Operator for Transmission Facilities meeting the criteria in 1.6 or 1.7.
Response: Thank you for your comments. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
Xcel Energy	No	We believe that 1.3 needs better definition. Specific criteria for designating generation facilities as required for reliability should be identified.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."		
Great River Energy	No	1.3 The criteria needs to be more clear on what is meant by "required for reliability purposes" 1.4 We suggest additional qualifying criteria such as "blackstart resources identified as critical to restoration in a regions restoration plan" 1.5 Suggest additional qualifying criteria "BES elements/facilities comprising the Cranking Paths..." For instance if there are multiple distribution subs within the Cranking Path are these now critical assets? Suggest additional qualifying criteria such as "Cranking Paths to critical units as identified in a region's restoration plan" 1.7 Is there a specific engineering basis for three? A better explanation is needed - does this mean upstream, downstream, radial, networked, etc.?

Organization	Yes or No	Question 2 Comment
		1.9 Please add to the standard the commonly accepted definition of a FACTS system and include it as a newly defined term since the definition of FACTS is not currently in the Glossary. 1.11 Please clarify who decides what "essential" is.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. There is no longer any NERC requirement to have a region restoration plan. Item 1.5 **–** There is no longer any NERC requirement to have a region restoration plan. Any substation may be considered a Critical Asset if it is in the Cranking Path. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.7 – In order to be more accurate in terms of the impact, the Drafting Team thought that it was more appropriate to refer to the number of connected transmission substations instead of lines connected to any particular transmission substation. The intent was to get away from the double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them. This includes upstream, downstream, radial and networked substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.9 – FACTS is defined by IEEE as: "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Commonly accepted terms and definitions do not require an insertion in the NERC Glossary. Item 1.11 – This is defined in NUC-001-2 Requirement 9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs."		
ITC Holdings	No	
Public Utility District No. 1 of Clark County	Yes	Attachment 1, part 1.14 would make a control center performing the functional obligation of a TOP a Critical Asset. This apparently would be the case even if a TOP's control center only performed these functions on facilities that are not critical. Small entities have in some cases been forced by Balancing Authorities and former Transmission Operators to register as TOPs. Many of these small entity TOPs operate systems with no assets that qualify as Critical Assets under any of the other Attachment 1 criterion. Some of these TOPs operate systems that do not qualify as Bulk Electric System facilities. It is unreasonable to designate these utilities dispatch centers as Critical Assets unless these dispatch centers actually control or operated Critical

Organization	Yes or No	Question 2 Comment
		Assets. Part 1.14 should be modified as follows:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator over any facilities determined to be Critical Assets as determined in Attachment 1, criterion 1.1 through 1.13.
Response: Thank you for your comments. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
TransAlta	Yes	It is an improvement using the bright-line approach to identify the critical asset instead of the RBAM. But there are some concerns in the criteria as described below. We will vote affirmative until the following concerns are properly addressed in the next draft. For the criterion 1.1, it mentions "generating units (including nuclear generation) at a single plant location". It is not clear what will be defined as a single plant location. Can the drafting team provide guidance for this to help the registered entity to classify the generating units properly? For the criterion 1.3, the Planning Coordinator or Transmission Planner can unilaterally decide the generation facility as required for reliability purposes without input from the registered entity. The registered entity has not option but comply with. The consequence would be the registered entity would spend a large amount of resources to comply with. We understand that there are some discussions in NERC about the cost recovery for the compliance, which may address this concern in the future. But at this stage, the registered entity has obligation to identify the critical asset. Neither the Planning Coordinator nor Transmission Planner has this accountability. Thus, to address this issue, one option is that the registered entity should be given the right to agree or disagree on any generation facility to be required for reliability purposes if the Planning Coordinator or Transmission Planner plans to do this. For this option, it is recommended adding "to which has been agreed by the responsible entity" at the end of this criterion. Another option is to clearly define "reliability purposes" in the standard, which the Planning Coordinator, Transmission Planner, and registered entity will all have to follow. For the criteria 1.6 and 1.7, transmission facilities should exclude the Generator Interconnection Facilities which was defined in this nerc project http://www.nerc.com/filez/standards/Project2010-07_GOTO_Project.html. The reason is that Generation Interconnection Facilities are the sole-use facility for the purpose of connecting the generating unit(s) to the transmission grid. Its criticality is directly related to the

Organization	Yes or No	Question 2 Comment
		criticality of the generation resources which are assessed against Criteria 1.1, 1.3. The criticality of these facilities should be differentiated from other transmission facilities. This issue was discussed in the draft guidance document. We think the appropriate wordings to clarify this should be put in to the standard, instead of addressing this in the guidance document, http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf. For the criterion 1.15, control center is not a defined term in the NERC glossary. In all existing FERC approved standard except CIP-002, all requirements with the control center wordings are applicable to BA, TOP, and RC. In the NERC CIPC approved guideline, "Security Guideline for the Electricity Sector: Identifying Critical Assets", there is a definition of control center. The draft guidance document http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf talks about the generation control center consideration. But we are still not clear what kind of facilities will be considered as the generation control center. We would like the drafting team to clarify the control center used for the generation.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 – The burden for identifying Critical Assets resides with the Responsible Entity that is the asset owner. The Planning Authority and/or Transmission Planner are not designating the asset as critical for CIP purposes; they are determining the unit to be necessary to avoid Adverse Reliability Impacts based on other NERC reliability standards. This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.6 –The drafting team believes "Transmission Facilities operated at 500 kV or higher" does not require any further qualification to clarify their role as components of the backbone on the Interconnected BES.

Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset any Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."

Item 1.15 – At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the

Organization	Yes or No	Question 2 Comment
Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect.		
Exelon	No	The revised criteria are acceptable in the sense that all generation is now treated equally, regardless of fuel type, and the specific cyber assets of concern are those with the potential for shutdown of multiple units in real-time.
Response: Thank you for your comments.		
N.W. Electric Power Cooperative, Inc.	Yes	CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability

Organization	Yes or No	Question 2 Comment
		Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. that control greater than 4,000MW.
Central Electric Power Cooperative	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the

Organization	Yes or No	Question 2 Comment
		BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. that control greater than 4,000MW.
Central Electric Power Cooperative	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not

Organization	Yes or No	Question 2 Comment
		occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. that control greater than 4,000MW.
M & A Electric Power Cooperative	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required then something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations on those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur, this control center, control system, backup control center, or backup control system can be exempted.

Organization	Yes or No	Question 2 Comment
		Bright Line is required for each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator, that controls greater than 4,000MW.
Sho-Me Power Electric Cooperative	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control

Organization	Yes or No	Question 2 Comment
		system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. that control greater than 4,000MW.
KAMO Power	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator that control greater than 4,000MW.
Associated Electric Cooperative, Inc.	Yes	CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
KAMO Electric Cooperative	Yes	The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
Northeast Missouri Electric Power Cooperative	Yes	The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
NW Electric Power Cooperative, Inc.	Yes	CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
Sho-Me Power Electric Cooperative	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
Northeast Missouri Electric Power Cooperative	Yes	The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
M&A Electric Power Cooperative	Yes	CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required then something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations on those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required for each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator that control greater than 4,000MW.
Associated Electric Cooperative, Inc.	Yes	CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
Associated Electric Cooperative, Inc.	Yes	Comments: CIP-002-4 - Attachment 1 Critical Asset Criteria The following are considered Critical Assets: 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. IF a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP.Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or

Organization	Yes or No	Question 2 Comment
		Transmission Operator. that control greater than 4,000MW.
AECI	Yes	1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. There is no technical basis or justification provided for the 1500MW criteria. If an entity has 4000 MW and is capable of proving that a loss of the 4000MW plant does not cause the BES to become unstable it should not be a Critical Asset. Therefore, suggested wording is: Each group of generating units (including nuclear generation) at a single plant location with its aggregate highest rated net Real Power capability of the preceding 12 months that through either testing or simulation can prove that a loss of the generating units causes an IROL. If a Bright Line criteria is required than something more reasonable that has an impact on the BES should be considered such as 4000MW. 1.6. Transmission Facilities operated at 500 kV or higher. There is no basis for this. It should state Transmission Facilities operated at 500 kV or higher that if rendered unavailable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities that operate at 500KV or higher with greater than 4,000 MW of flow. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. There is no technical basis for this requirement. Suggestion: Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that if rendered inoperable violate one or more Interconnection Reliability Operating Limits (IROLs). Bright Line criteria - Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations that have greater than 4,000 MW of flow into the facility. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. Based on the way this is written there are Local Control Centers that perform functional obligations for the TOP. I am basing functional obligations as those that are defined in the NERC functional model for a TOP. Suggestion: Add a note that if through testing or simulation a control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator is completely destroyed and all breakers on the BES are opened and a violation of one or more Interconnection Reliability Operating Limits (IROLs) does not occur this control center, control system, backup control center, or backup control system can be exempted. Bright Line is required than Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. that control greater than 4,000MW.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.1 - The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method by providing bright line criteria. Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Items 1.6 and 1.7 – The SDT does not feel that a power flow analysis (impact-based or risk-based) to determine line flows for the bright line criteria will lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
LCRA Transmission Services Corporation	Yes	1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. If a multiple path option exists from the Black Start Resource to a Next Start unit, does a Critical Path have to be designated? To clarify, the criteria states "The Facilities comprising the Cranking Paths... up to the point where multiple path option exist." If LCRA has multiple paths originating directly at the Black Start Resource, either path could be used as a cranking path. Therefore, neither path would be considered critical. Could this be clarified? 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. 1) Does this includes radial interconnections? This is a question because a 345 kV station could be interconnected to 3 other stations, but one of the interconnections could be a radial 345 kV line connected to a generator.2) Is there a distance requirement for the interconnection? This is a question because a 345 kV station could be interconnected to 3 other stations, but one of the interconnections could be a 345kV bus connected to another station a few feet away.
Response: Thank you for your comments. Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification		

Organization	Yes or No	Question 2 Comment
of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. Based on your example, neither path would be identified as a Critical Asset. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."		
United Illumiinating	Yes	Change 1.3 to Each generation Facility that the Planning Coordinator or Transmission Planner has designated as required to avoid one or more reliability criteria violations. Change 1.8 to Transmission Facilities at a single station location that the Planning Coordinator or Transmission Planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations. The reason for the change is that destruction or misuse of equipment does not violate an IROL, the destruction causes the IROL on another interface to be violated. Also since TPL and PC are not listed as applicable entities to the standard, we feel it appropriate to specifically state that it is the PC and TPL that determine these facilities and no the Transmission Owner; Transmission Owners do not conduct the studies required to determine IROL. Change 1.11 to Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements. NPIR is a broad based document with many requirements. IT would be helpful if the standard brightly identified what is critical to a nuclear plant. We believe it is the preservation of off site power for plan safety. Change 1.12 to Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROLs) violations for failure to operate as designed. The reason for the change is that the misuse of an SPS would cause an IROL to be violated, and not all SPS are required to protect for IROL so the the standard should only apply to those that are installed to protect for IROL violations.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed."		
Constellation Energy Commodities Group	Yes	Has there been any discussion about the enforcement of criteria versus a requirement in relation to the version 4 draft? The standard describes Attachment 1 as criteria that are to be applied by an entity to develop a Critical Asset list. Criteria have historically been viewed, in my experience, as guides but not Requirements. Has the drafting team stated why they are not clearly documenting that an entity that operates assets meeting the description in Attachment 1 is required to be on the entities Critical Asset list? Failure to define terms that are used in the Attachment will also continue to create confusion: Transmission Facility, control center, and control system need to be defined to ensure consistent application of the criteria in the attachment. 1.5 In an effort to add clarity, it should be changed to read "The facilities comprising the Cranking Path and initial switching requirements from the Blackstart Resource to the first interconnection point of the generation facility to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. 1.11 Should be removed. Criticality of facilities should not be fuel specific. 1.13 The threshold should be consistent with that in 1.1. Automatic should be defined as requiring no human interaction to enact load shedding. 1.14 The current use of the term "control center" assumes that every control center fits into a certain box (i.e. remote breaker operations, remote generation start up/shut down, and load shed), but is applied to centers with little to no impact on system reliability. If there is an asset that can affect limits that are critical to the RC and TOP footprint then the protections should be in place. However, for generation assets and their interconnection facilities that do not have the ability to create SOL or IROL conditions, it is not practical to require CIP control measures. The role of such a control center in this case is generally just to capture a data

Organization	Yes or No	Question 2 Comment
		point for producing better system models. Such data is not for contingency planning or real time operational response awareness. A complete loss of data does not modify how the RC and TOP respond to the customers therefore, likewise a manipulation of the data would not trigger a BES reliability concern. For systems that cannot operate equipment remotely, applying CIP controls would be costly and provide only marginal reliability improvement at best. 1.15 Defining the area as 'in a single interconnection' is extremely broad and should be narrowed down to a maximum area of Balancing Authority. What other control centers /back-up control centers does the drafting team expect to capture that would not be captured under 1.14? How will they define generator control? The "control generation greater than an aggregate of 1500 MWs" criteria should be restricted to the amount of generation that could be controlled in a 10 minute period (NERC Control Performance Standard). The MW change occurs using pre-determined ramp capability limits.

Response: Thank you for your comments.

CIP-002-4 Requirement R1 states "Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Attachment 1 starts with "The following are considered Critical Assets:" The combination of these two make the criteria in Attachment 1 part of the requirement. Any asset meeting any criterion in Attachment 1 must be listed as a Critical Asset.

At this time, the SDT is choosing not to add Transmission Facility, control center, and control system to the NERC Glossary. We feel defining these term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets.

Item 1.13 – This criterion has been changed to "System(s) or facilities that perform automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the

Organization	Yes or No	Question 2 Comment
Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 – This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection.". Criterion 1.14 does not include generation control centers and generation backup control centers		
Sierra Pacific Power d/b/a NV Energy	No	We appreciate the efforts of the drafting team to identify in Att 1 those Assets that would be deemed Critical. There are a few areas for which we would like the SDT to reconsider: 1.3 Reliability Must-Run Generation - The language here appears to lack precision. For instance, a Transmission Planner may designate a particular generating plant to be required for reliability purposes during specific system conditions, such as above a certain demand level or path flow level. These sorts of occasional must-run situations should not be treated as Critical Generation. Critical should be reserved for instances where the reliability must-run condition is prescribed by the Planner on a perpetual basis. 1.4 The inclusion of "Each Blackstart Resource" identified in the TOP restoration plan may be overboard. In many instances, entities will include multiple options for blackstart resources in their restoration plans, and with this language, all of the blackstart resources that are even mentioned in one's plan will be deemed Critical. Suggest changing this parameter to the "primary blackstart resource identified in the TOP restoration plan." The point is that not every one of these blackstart resources should be deemed Critical. 1.7 We would like to see some discussion of the rationale for including 300kV and above stations with three or more connections. Consider the scenario where one or more of these "connections" is radial. Would this station really rise to the level of Critical in that case? We suggest raising the criterion to four or more non-radial connections. 1.15 Need some explicit criteria for what constitutes a "control center" vs a "control room" with respect to generating stations.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart		

Organization	Yes or No	Question 2 Comment
Resources. Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.15 – Thank you for your comment. This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection."		
SDG&E	Yes	Comment on 1.3: Need to ensure PC or TP have notified Transmission Operator and Generator Owner. Suggested wording additions "... designates to the Transmission Operator and Generation Owner as ...". Comment on 1.4: As worded, the language will discourage a TOP from having additional backup Blackstart Resource. Suggested wording additions "Each primary Blackstart resource identified in the Transmission Operator's restoration plan." Comment on 1.5: As worded, the language will discourage a TOP from having additional backup Blackstart Resource. Suggested wording addition "The Facilities comprising the Cranking Paths and initial switching requirements from the primary Blackstart Resource ..." Comments on 1.14. Suggest rewording to avoid confusion at Control Centers. Change wording to "Each control center, backup control center, or other facility housing control systems used to perform...."
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. No Transmission Operator is required to designate any "primary" Blackstart Resource. Therefore the language cannot be changed to your suggestion. Item 1.5 – No Transmission Operator is required to designate any "primary" Blackstart Resource. Therefore the language cannot be changed to your suggestion.		

Organization	Yes or No	Question 2 Comment
This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
Central Lincoln	No	1.1 Central Lincoln supports the APPA Comments:APPA and others commented on the CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. APPA commends the SDT for their attempted to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. The use of an average of the Contingency Reserve numbers from all the regions bases the bright-line on what the regions consider operationally significant. We understand that NERC standards are a minimum requirement and regions can look at their own operating criteria and determine if they need additional protection at lower Megawatt bright-lines. APPA is concerned that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2. 1.2 Central Lincoln supports the APPA Comments:APPA does not have a comment on criteria 1.2 at this time. 1.3 Central Lincoln supports the APPA Comments:â€,APPA commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. APPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: "Adverse Reliability Impacts" will help clarify which units should be in this category.We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. APPA proposes the following rewording of criteria 1.3:"1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer."

Organization	Yes or No	Question 2 Comment
		1.4 Central Lincoln supports the APPA Comments:APPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). APPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, APPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW.We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan. We further support inclusion of "ALL Blackstart Resources" only when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal. 1.5 Central Lincoln supports the APPA Comments:APPA commends the SDT on differentiating between a single Cranking Path as a critical facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. APPA does request clarification of criteria 1.5: Where does this point of multiple paths lay in the electrical system? Does this include only the Generator Step-up Transformer, or does it include the whole substation where multiple transmission paths depart to a single generator? Also, APPA suggests that the

Organization	Yes or No	Question 2 Comment
		SDT change “switching requirements” to “switching equipment.” 1.6 Central Lincoln supports the APPA Comments:APPA does not have a comment on criteria 1.6 at this time. 1.7 Central Lincoln supports the APPA Comments:APPA believes that criteria 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations).APPA also supports the MRO standard review team proposal to adopt a power flow based bright-line rather than whether the station is connected to three or more other stations:Under TPL-001, the Planning Coordinator or Transmission Planner already performs annual near-term power flow assessment and this particular assessment would be based on the forecasted peak conditions using Category A of Table 1 of the standard.Proposed rewording of criteria 1.7:1.7. Each Transmission Facility operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher where the TPL peak load studies of the Planning Coordinator or Transmission Planner identifies the sum of the incoming power flows or the sum of the outgoing power flows to exceed 1500 MW. 1.8 Central Lincoln supports the APPA Comments:APPA believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). 1.9 Central Lincoln supports the APPA Comments:APPA believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). 1.10 Central Lincoln supports the APPA Comments:APPA does not have a comment on criteria 1.10 at this time. 1.11 Central Lincoln supports the APPA Comments:APPA does not have a comment on criteria 1.11 at this time. 1.12 Central Lincoln supports the APPA Comments:APPA understands there are utilities within the NPCC region that have SPS type 3 systems that only protect local areas. We seek verification from the SDT that the SPS they refer to in criteria 1.12 is for wide area protection only. 1.13 Central Lincoln supports the APPA Comments:APPA believes the SDT’s change in wording of criteria 1.13 will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. As written, this criteria designates as a critical asset various control systems that by themselves could not cause instability or uncontrolled separation of the BES.APPA offers the following alternatives for rewording 1.13:1.13 Common control system(s) configured to perform automatic load shedding of 300 MW or more within 15 minutes.APPA can accept the bright-line of 300 MW if the wording is changed to that stated above, but we still see this bright-line as an

Organization	Yes or No	Question 2 Comment
		arbitrary threshold based on a quantity that has no BES operational significance. Rather, 300 MW is a DOE threshold for electric event reporting. 1.14 Central Lincoln supports the APPA Comments:APPA is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15.APPA offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. APPA cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability or uncontrolled separation of the BES.However, we will support inclusion of "ALL BA and TOP control centers" only when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal.Additional Central Lincoln Comments: The terms "control center," "control system," "backup control center," and "backup control system" all need to be clearly defined. While there is guidance on the subject, guidance cannot be audited to. Some of the guidance would suggest a cell phone capable of receiving text message alarms from two or more BES elements qualifies as a CCA and subject to CIP-003 through 009. 1.15 Central Lincoln supports the APPA Comments:In the NERC Draft CIP-002-4 webinar it was stated that a control center in criteria 1.15 is understood to be controlling multiple units. APPA recommends that the SDT clarify the wording in criteria 1.15 to coincide with this understanding: 1.15 Each control center or backup control center used to control multiple generation units identified as Critical Assets designated under criterion 1.3 or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. 1.16 Central Lincoln supports the APPA Comments:APPA believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Response: Thank you for your comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants

Organization	Yes or No	Question 2 Comment
that operate near the 1500 MW bright line. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.7 – The SDT agrees to change "stations" to "stations or substations." The SDT does not believe that power flow based bright-line criteria that is based on MW flows into or out of a substation would meet the objective of uniform application of Critical Asset identification across all entities. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. The present wording is appropriate. The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 - The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.12 – Since this item only applies to SPSs that have IROLs associated with them, local area SPSs are not included. This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."		

Organization	Yes or No	Question 2 Comment
Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
National Rural Electric Cooperative Association (NRECA)	Yes	1. A general comment is that there is no technical justification provided for the proposed criteria. The "Rationale and Implementation Reference Document" does not provide technical justification, but rather provides more of an opinion of the drafting team. To the extent possible, there should be technical justification for the proposed criteria that stakeholders can review. 2. NRECA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). NRECA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a Critical Asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, NRECA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. 3. In item 1.7 the statement regarding "three or more other transmission stations" is confusing. A better

Organization	Yes or No	Question 2 Comment
		explanation is needed -- does this mean stations upstream, downstream, networked or radial? 4. In item 1.14 the term "control center" must be defined, especially when dealing with the significance of the requirements of this standard. Using an undefined term here is inappropriate. 5. In item 1.14 its states that all RC, BA and TOP control centers, etc., are Critical Assets. While NRECA agrees with this as it relates to RCs, we do not agree with this as it relates to all BAs and TOPs. In the draft CIP-010 there was high, medium and low criteria which in many instances appropriately matching CIP requirements to the level of risk certain assets potentially present to the BPS. NRECA strongly believes that the CIP-002-4 standard requirements for smaller BAs and TOPs should match the lower level of risk to BPS reliability that these smaller BAs and TOPs potentially present. Similar to the 1500MW size criteria that is included in item 1.15 for generator control centers, there should be size criteria for the smaller BAs and TOPs. The drafting team should modify item 1.14 to state that all control centers with a peak demand above 2000MW (same as medium criteria in draft CIP-010) shall be designated as a Critical Asset. This is the lowest NRECA could support and also recommend its members to support. We firmly believe that this would capture all of the control centers that truly have a material impact on the reliability of the BPS. 6. Related to the Critical Asset Criteria, there should be a provision in the standard that provides a process for an entity to technically demonstrate that even though the criteria identifies some of their assets as Critical Assets, their assets (or a portion thereof) do not meet the definition of a Critical Asset and should be excluded from applicability of CIP-003 through CIP-009.

Response: Thank you for your comments.

The SDT believes information provided in the guidance document (posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf) provides sufficient technical justification for each criterion.

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other

Organization	Yes or No	Question 2 Comment
transmission stations or substations." Item 1.14 – At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.		
Tampa Electric	No	
MEAG Power	Yes	MEAG supports the APPA's comments submitted to the NERC CIP standard drafting team.
Response: Thank you for your comments. Please refer to the response to APPA's comments.		
FirstEnergy Corp	Yes	Overall FE agrees with the fundamental concepts of the Attachment 1 Critical Asset Criteria. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. 1) Criterion 1.8 currently states "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014.C.) A possible misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say "Transmission Facilities at a single station location ..." not all transmission facilities at a single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8:"1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates

Organization	Yes or No	Question 2 Comment
		the need for an Interconnection Reliability Operating Limit (IROL)."The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements" Clarity needed: The term "essential" is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the following change for 1.11:"1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements." 3) Criterion 1.5 currently states "The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist." FirstEnergy suggests replacing the word "multiple" with "two or more" for clarity. 4) Criterion 1.14 currently states "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." FirstEnergy suggests removing the text "control system" and "or backup control system" for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the "control center" then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase "control system" is vague.

Response: Thank you for your comments.

Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Organization	Yes or No	Question 2 Comment
Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."		
Minnesota Power	Yes	Criterion 1.1: The phrase "single plant location" is undefined. It is unclear if this means at a single street address or within some number of miles. Criterion 1.3: Criterion 1.3 should be modified to clarify that it is not meant to create the need for new or different planning models to be used by the Planning Coordinator or Transmission Planner. Rather, the verbiage should be clear that the Planning Coordinator or Transmission Planner has the opportunity to identify Generation Facilities that have been historically required to support the BES. Criterion 1.10: The phrase "loss of the assets" in criterion 1.10 is vague, leaving open for interpretation to what level a "loss of the assets" might mean. Criterion 1.10 also specifies "Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system..." where such assets are included in Criterion 1.1 or 1.3. In reality, there may be multiple paths from an aggregate station to the transmission system. To accommodate the above concerns, Minnesota Power suggests eliminating criterion 1.10 and modifying criterion 1.3 as follows: "1.3 Each generation Facility or Transmission Facility providing the generator interconnection that the Planning Coordinator or Transmission Planner has designated as required to avoid one or more reliability criteria violations." Criterion 1.8: The phrase "single station location" is undefined. It is unclear if this means at a single street address or within some number of miles. In addition, criterion 1.8 should be clear that it is not meant to require the Planning Coordinator or Transmission Planner to create new or different planning models. Rather, they should continue to use the legacy planning models as specified in FAC-010, FAC-011 and FAC-014. Minnesota Power recommends the following language for criterion 1.8, with further clarification of the term "single station location"."1.8 Transmission Facilities at a single station location that the Planning Coordinator or Transmission Planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limits (IROLs) violations." To maintain consistency with the suggested changes to criterion 1.8, Minnesota Power recommends changing criteria 1.9 and 1.12 as follows: "1.9 Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limits (IROLs) violations.""1.12 Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection

Organization	Yes or No	Question 2 Comment
		Reliability Operating Limits (IROLs) violations for failure to operate as designed." Criterion 1.14: Minnesota Power recommends rewording criterion 1.14 as follows for consistency with criterion 1.15: "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator."

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generators classified as Critical Assets. Any Transmission Facility the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

Organization	Yes or No	Question 2 Comment
Manitoba Hydro	Yes	Comments: Criterion 1.5: Suggest changing wording from "... and initial switching.." to " ... which meet the initial switching ...". It is unclear what "multiple path" means. Criterion 1.13: Distribution Provider is not included in the Applicability section, and therefore 1.13 does not apply to Distribution control systems, including Distribution Control Centres. Please clarify what "automatic" means, whether operator initiated or not operator initiated. It is unclear if the 300MW is shed simultaneously or in blocks over time. The loss of generation or the loss of load are analogous in their reliability impact on the BES, thus criterion 1.13 using a 300 MW threshold seems inconsistent with criterion 1.1 using a 1500 MW threshold.
Response: Thank you for your comments. Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."		
American Transmission Company	Yes	ATC offers the following suggestions for Attachment 1: 1.1 Support EEI's suggestion. The phrase "single plant location" is undefined. Suggest the term be defined by the SDT. 1.2 Similar to 1.1; define "single location". Does this include reactive resources connected to the same kV class or across kV classes in a single substation? 1.3 Support EEI's suggestion. Modify requirement to indicate the facilities that have been historically required to support the BES. 1.4 None 1.5 None 1.6 None 1.7 If the interconnection to another substation consists of a transformer to a lower kV class, does the language "interconnection at 300 kV" apply to the high side winding voltage of the transformer or the low side winding voltage of the transformer?

Organization	Yes or No	Question 2 Comment
		1.8 Support EEI's suggestion. "...single station location" is undefined. Add clarity by indicating the Planning Coordinator and Transmission Planner determine and communicate IROL's in the planning horizon per FAC-014. Also, recommend adding the word "All BES" before "Transmission Facilities" at the beginning of the sentence if this is the intent of the language to avoid ambiguity. 1.9 Support EEI's minor word changes. Clarification should be made if this covers all FACTS devices in a substation even if they connect at different points or are at different kV levels. 1.10 Clarification should be made if this item covers only the Transmission Facilities defined as "Interconnection Facilities" in the Midwest ISO tariff or if more than that is covered. If clarification is not made, entities may misunderstand the terms used in this item. 1.11 Support EEI's suggestion. Remove the ambiguous term "essential" and insert Transmission Facilities "providing offsite power requirements as identified in the" NPIR. 1.12 Support EEI's suggestion. Revise wording so that SPS...that "would cause" one or more IROL "violations for failure to operate as designed." 1.13 None 1.14 None 1.15 None 1.16 Support EEI's suggestion. Insert "Any additional assets owned by the Responsible Entity.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.2 – Please see response to Item 1.1 for clarification on "single location."

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.7 – The "interconnection at 300 kV" would not apply to any substation connected at less than 300 kV. In addition, any lines leaving a substation at less than 300 kV would not be classified as a Critical Asset per criterion 1.7. In short, language applies to any transformer winding 300 kV or more. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other

Organization	Yes or No	Question 2 Comment
transmission stations or substations." Item 1.8 – Please see response to Item 1.1 for clarification on "single location." FAC-014-2 requires all Reliability Coordinators and Planning Authorities to establish IROLs consistent with its SOL methodology. They are the only ones who can establish IROLs. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.10 – Please refer to the NERC Glossary definitions of Transmission and Facility. Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
Ameren	Yes	We believe that impact on the BES should be evaluated for the Critical Asset using the performance requirement contained in the existing mandatory standards. This would provide consistency between CIP-002 and other standards. In this regard, we suggest that for the facilities identified in the bright line criteria, perform powerflow and stability simulations to assess the impact to the BPS of the outage of these facilities, similar to the tests performed for TPL-003 and 004. If there is an impact (that is not meeting the performance criteria), then the facility is to be considered as critical. If there is no such impact, then the facility is not be considered as critical. If there is a concern for a multi-prong attack, then similar reliability assessment should be performed for such scenarios. We offer some comments/suggestions and also have some questions to the bright line criteria (Attaachment 1): The term "Facilities" should be changed to "substations and switchyards" throughout Attachment 1 as NERC glossary of terms include "lines" in the definition also. Is it SDT's intention to include hundreds of miles of lines as critical asset? The term "single station location" and "single plant location" used throughout Attachment 1 need to be defined to avoid confusion whether a single location mean one building or several buildings or stations within a defined geographical boundary or a fenced area. 1.1 - Are there any reliability impact studies to support 1500 MW? We believe that several events larger than this number have occurred and the BES has performed as designed, without any loss of load, or significant

Organization	Yes or No	Question 2 Comment
		impact on reliability. 1.6 - We disagree that all transmission facilities operated at 500 kV or greater are "critical". Again, system studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.7 - We disagree that all transmission facilities that are operated at 300 kV or above and are interconnected with three or more transmission substations are "critical. System studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.8 - Wording for this criterion should be changed to "Transmission substations and switchyards that the Planning Coordinator or Transmission Planner designates that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL). This change would make this criterion consist with FAC-010/FAC-014.1.12 - We believe that the criterion reads ok, but the rationale document for this criterion implies that purpose of SPS/RAS is to prevent disturbance that would result in excursion beyond IROLs. This may not be true in all cases. 1.13 - Wording for this criterion should be changed to "Common control system(s) capable of performing automatic load shedding of 300 MW or more with a single operation". 1.15 - Same comments as for 1.1 above. 1.16 - Wording for this criterion should be changed to "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include."

Response: Thank you for your comments.

The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The SDT does not feel that a power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry.

A transmission Line can be considered a Critical Asset if it meets the criteria in Attachment 1. It would then be evaluated for possible Critical Cyber Assets, which would be afforded the cyber security protection outlined in CIP-003 to CIP-009. It is not the Critical Asset that falls under CIP-003 to CIP-009, but the Critical Cyber Asset.

The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a

Organization	Yes or No	Question 2 Comment
single plant. Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Items 1.6 and 1.7 – You propose to add the criteria that the Responsible Entity can determine through a risk based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The SDT does not feel that a power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.15 –In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections. Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
BGE	Yes	There is more clarity in the definition of Critical Asset through the 16 criteria. Specific improvement items:- Clearly state in the Guidance Document the basis for each of the first 15 criteria (1.1 to 1.15), Responsible Entity should define 1.16. The acceptable methods of "deeming appropriate" should be described in the Guidance Document. In 1.8, 1.9 and 1.12 define the IROLs as those determined in year-out planning studies Criteria for common control system (1.13) based on system reliability, not a NERC reporting figure. This needs to be consistent with the criteria in 1.1 (1500 MW). Clarification is required in the Guidance Document on the definition of "automatic load shedding". Term clearly states "no human intervention".
Response: Thank you for your comments.		

Organization	Yes or No	Question 2 Comment
The SDT believes information provided in the guidance document (posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf) provides sufficient technical justification for each criterion. Items 1.8, 1.9, and 1.12 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. They are the only ones who can establish IROLs. Criterion 1.8 has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.9 has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."		
Beaches Energy Services (of City of Jacksonville Beach, FL)	Yes	1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. BES Comments: BES commends the SDT for their attempt to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. However, we continues to have the comment FMPA submitted in CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. BES is concerned that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1, R2. SDT Proposed:1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. BES Comments: BES believes that this "bright line" is arbitrary and instead suggests combining this with 1.9. There is no significant difference between the MVARs provided by FACTs devices and those provided by a power plant and it makes sense to treat them both in the same fashion. SDT Proposed:1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes. BES Comments: BES commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. We suggest that the designation of facilities be based on studies conducted under the TPL Standards to justify the designation. Also, the use of NERC Glossary of

Organization	Yes or No	Question 2 Comment
		term: “Adverse Reliability Impacts” will help clarify which units should be in this category.We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate "Must Run" units for temporary situations, so this must be clarified within the criteria. BES proposes the following rewording of criteria 1.3:”1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer.” SDT Proposed:1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. BES Comments: BES is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). We understand that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator’s restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective restoration plan, reducing the plan’s overall robustness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource’s actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, we would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports.We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13:1.4 Each Blackstart Resource identified in the Transmission Operator’s restoration plan, which meet either of the following criteria:1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW. We believe this approach should provide a better measure of a Blackstart Resource’s potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator’s restoration plan. SDT Proposed:1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan

Organization	Yes or No	Question 2 Comment
		up to the point on the Cranking Path where multiple path options exist. BES Comments: BES commends the SDT on differentiating between a single Cranking Path as a critical facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. We suggest that the SDT change "switching requirements" to "switching equipment." SDT Proposed:1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. BES Comments: BES believes that criteria 1.7 is rather arbitrary and suggests use of TPL-004-0 Category D testing and to combine 1.7 with 1.8. Does loss of a substation result in an IROL or Adverse Reliability Impacts? Doing so can also remove the voltage class limit. It is also unclear from the wording whether the entire substation is a Critical Asset, or whether each Facility connected to that substation is a Critical Asset. We suggest the entire substation. It is also unclear for substations that have two voltage levels (e.g., a 345 kV to 115 kV substation), whether the entire substation should be considered, or just one voltage level. We suggest one voltage level as discussed in the existing TPL-004 standard. SDT Proposed:1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). BES Comments: BES believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse Reliability Impact would be beneficial. Proposed rewording of criteria 1.8:1.8. Transmission Facilities at a single station or substation that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs) or can cause an Adverse Reliability Impact as a result of extreme contingency loss of substation testing as part of the TPL standards or as determined by the Reliability Coordinator. SDT Proposed:1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). BES Comments: BES believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). Also the use of term Adverse Reliability Impact would be beneficial. SDT Proposed:1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered

Organization	Yes or No	Question 2 Comment
		unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). BES Comments: BES believes that adding the phrase “or can cause an Adverse Reliability Impact” would be beneficial. SDT Proposed:1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. BES Comments: BES believes that the 300 MW is arbitrary and seems based more on reporting requirements than on true reliability impacts. Also, it should not matter whether loss of load is caused by an “automatic” system or not. In addition, the power system is more resilient to loss of load than loss of generation; hence, by using the same threshold as is used in 1.1, we are actually being quite conservative. BES offers the following alternatives for rewording 1.13:1.13 Common control system(s) that can result in a loss of load equal to or greater than the reserve sharing requirements of the Reserve Sharing Group within 15 minutes. SDT Proposed:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. BES Comments: BES is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15.BES offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system that can:1.14.1 Cause a loss of generation or load greater than the reserve sharing requirements of the Reserve Sharing Group1.14.2 That if manipulated, can cause an Adverse Reliability Impact as determined through planning studies. BES cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability, cascading or uncontrolled separation of the BES. SDT Proposed:1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. BES Comments: With the proposed revision to 1.14, this 1.15 would no longer be required. SDT Proposed:1.16. Any additional assets that the Responsible Entity deems appropriate to include. BES Comments: BES believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets.

Organization	Yes or No	Question 2 Comment
		We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Response: Thank you for your comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line.

Item 1.2 – The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality. FACTS devices in 1.9 are specifically related to IROLs, whereas the reactive resources in 1.2 are not limited to IROL applications.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.7 – The SDT agrees to change "stations" to "stations or substations." The SDT does not believe that power flow based bright-line criteria (i.e. using TPL-004-0) would meet the objective of uniform application of Critical Asset identification across all entities. The term Transmission Facilities can be applied to either the entire substation or each Facility or group of Facilities connected to that substation, as determined by the entity. This would allow an entity which has multiple voltage levels at a single substation to either declare the entire substation as a Critical Asset or only the portion of the substation that qualifies under criterion 1.7. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."

Item 1.8 –The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.9 - The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of

Organization	Yes or No	Question 2 Comment
Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.12 – By limiting the scope of Criterion 1.12 to IROLs, Adverse Reliability Impacts are covered as well. This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
We Energies	Yes	We suggest that the functional entities Planning Coordinator and Transmission planner be added to the applicability section. Feedback on specific criteria as follows: 1.1, We request clarification on the phrase "single plant location". This phrase is not defined and it is not clear what level of proximity of generators would be considered a "single plant location". Rather than discuss this in terms of geography (location), we feel it would be better to discuss in terms of "Each group of generating units (including nuclear generation), operated using common cyber control systems other than the Control Centers identified in 1.14 and 1.15, with an aggregate...". 1.3, We suggest the wording: "Each generation facility designated by the Planning Coordinator or Transmission Planner as required to avoid one or more reliability criteria violations". 1.4, The blackstart units deemed critical should be only those identified by the Transmission Operator to meet the minimum critical blackstart requirement. The resulting suggested wording would be: "Each Blackstart Resource identified in the Transmission Operator's restoration plan required to meet the minimum critical blackstart requirement". 1.8, We suggest the wording: "Transmission Facilities at a single location that the Planning Coordinator or

Organization	Yes or No	Question 2 Comment
		Transmission planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations". 1.9, We suggest similar wording: "...unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations". 1.11, We suggest the following wording: "Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements". 1.12, We suggest the following wording: "...unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed". 1.14, We suggest this be made consistent with 1.15, i.e. "Each control center, or backup control center, used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator". 1.16, We suggest the following wording: "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include".

Response: Thank you for your comments.

Since there is no Requirement that applies to the Planning Coordinator or the Transmission Planner, it is not appropriate to include them in the Applicability section.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.

Item 1.8 – According to FAC-014-2 IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of

Organization	Yes or No	Question 2 Comment
Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
City Utilities of Springfield, MO	Yes	SPRM agrees with the comments by the APPA Task Force, incorporated herein by reference. SPRM has additional specific comments as noted below. 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. SPRM agrees with the comments from the APPA Task Force. 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. SPRM does not have a comment on criteria 1.2 at this time. 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes. SPRM agrees with the comments from the APPA Task Force and will add an additional request for the drafting team to consider using this criterion to identify critical transmission. SPRM proposes the following rewording of criteria 1.3:1.3 Each transmission or generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer. 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. SPRM generally

Organization	Yes or No	Question 2 Comment
		agrees with the comments from the APPA Task Force. However, SPRM proposes the following exception to the APPA rewording of criteria 1.4:1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3. 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. SPRM agrees with the comments from the APPA Task Force and additionally will suggest the following rewording of criteria 1.5:1.5. The Facilities comprising the Cranking Paths and initial switching equipment from the Blackstart Resource identified in 1.4. to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. 1.6. Transmission Facilities operated at 500 kV or higher. SPRM would like to recommend that the drafting team verify that all transmission operated at 500 kV or higher is truly critical. Otherwise, SPRM will suggest that our proposed changes in criteria 1.3.would identify all transmission, regardless of voltage, that is critical to the reliable operation of the Bulk Electric System. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. SPRM generally agrees with the comments from the APPA Task Force and additionally would like to recommend that the drafting team verify that all transmission identified in this criteria is truly critical. Otherwise, SPRM will suggest that our proposed changes in criteria 1.3 would identify all transmission, regardless of voltage or interconnections, that is critical to the reliable operation of the Bulk Electric System. 1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).SPRM agrees with the comments from the APPA Task Force. 1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). SPRM agrees with the comments from the APPA Task Force. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3. SPRM would like the drafting team to clarify if the "Transmission Facilities" is the line connecting the generator to the bus in the substation, or is it the whole substation where the generator is connected? 1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements. SPRM would like to recommend that the drafting team verify that all transmission identified in this criteria is truly

Organization	Yes or No	Question 2 Comment
		critical. Otherwise, SPRM will suggest that our proposed changes in criteria 1.3. would identify all transmission, regardless of voltage or interconnection, that is critical to the reliable operation of the Bulk Electric System. 1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). SPRM agrees with the comments from the APPA Task Force. 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. SPRM agrees with the comments from the APPA Task Force. 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. SPRM agrees with the comments from the APPA Task Force. 1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. SPRM agrees with the comments from the APPA Task Force. 1.16. Any additional assets that the Responsible Entity deems appropriate to include. SPRM agrees with the comments from the APPA Task Force.

Response: Thank you for your comments. Please refer to the response to APPA's comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12 month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright line.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart

Organization	Yes or No	Question 2 Comment
Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.6 –The drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES. Item 1.7 – This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include a substation or the line connecting the generator to the bus in the substation. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3." Item 1.11 – This is defined in NUC-001-2 Requirement 9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs."		
National Grid	Yes	National Grid proposes to include the class of assets - generation, transmission, and control centers against each criterion in attachment 1. This will help entities to clearly identify which requirements fall under different classes of assets. For example - 1.5 The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. (Generation, transmission)
Response: Thank you for your comments. The Applicability section of the standard specifies what NERC Registered Entities the standard applies to. All Requirements apply to all Entities listed in the Applicability section.		
Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
Response: Thank you for your comments. Please refer to the response to MRO NERC Standards Review Subcommittee comments.		
Southwest Power Pool Regional Entity	Yes	Black start overall is not well understood. Black start should be defined as starting the entity's generation resources to the point that load can be served (not to be confused with bringing on load to balance generation during the black start sequencing). This is often more than starting the first "black start" combustion turbine unit to start a thermal unit. Unless that black start unit has sufficient capacity to start individually every other generation resource in the entity's footprint that is not self-starting, additional generation is required even if not specifically identified as a black start resource in the entity's restoration plan.

Organization	Yes or No	Question 2 Comment
		Consider declaring DC Tie substations as Critical Assets. Automated load shedding systems capable of shedding 300 MW or more should be considered Critical Assets regardless of the time it takes for the system to shed the load. Defining a 15 minute window is unnecessary and could result in disagreement between the entity and the auditor over whether the impact could occur within the fifteen minute versus a longer period. Removing the 15 minute criteria resolves that potential ambiguity. Additionally, please accept and consider the following comments that do not directly apply to any of the questions in the comment form. I have no other way to bring these comments to the drafting team's attention. M1: Measure M1 should be modified to state “The Responsible Entity shall make available its approved list of Critical Assets as specified in Requirement R1.” (addition of the word "approved") M2: Measure M2 should be modified to state “The Responsible Entity shall make available its approved list of Critical Cyber Assets as specified in Requirement R2.” (addition of the word "approved") M3: Measure M3 states “The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.” This measure should be modified to state “The Responsible Entity shall make available its approval records as specified in Requirement R3.” (Removes expectation of annual-only approval and requires any modification to the CA or CCA list to be approved) The Compliance Enforcement Authority obligations (Section D.1.1) fail to identify who is the Compliance Enforcement Authority for Responsible Entities that do perform delegated tasks for their Regional Entity. The Responsible Entity data retention requirement (Section D.1.4.1) should be modified to require records to be kept since the effective date of the standard or the most recent scheduled audit of this version of the standard, whichever is a shorter period of time. This is in keeping with NERC Compliance Process Bulletin #2009-005 'Current In-Force Document Data Retention Requirements for Registered Entities'. A similar modification should be made to CIP-003-4 through CIP-009-4. (Entities are already expected to retain all evidence in support of the annual, or in the case of the CIP standards to date, semi-annual self certification, so this is not an undue burden. Retention of records with the exception of specific information with a prescribed shorter retention, such as logs, will allow the CEA to verify sustained compliance with the standards over the full audit period. And, in the case of the logs, the entity will need to maintain some sort of evidence that logs were retained for at least 90 days, although retention of the actual logs is not required.)

Response: Thank you for your comments.

Item 1.4 – A Blackstart Resource is defined as “A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator’s restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator’s

Organization	Yes or No	Question 2 Comment
restoration plan." The SDT believes that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. Concerning DC Tie substations, we thank you for your proposal and will take it under consideration for future revisions. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." M1 – There is no requirement in R1 to have the list approved M2 – There is no requirement in R2 to have the list approved M3 – Has been modified to "The Responsible Entity shall make available its records of approvals as specified in Requirement R3." CEA info – Thank you for your comment. The appropriate clarification has been made. Data retention – Thank you for the comment. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The suggested changes to the data retention requirement will be made in a subsequent version of the CIP standards.		
Indianapolis Power & Light	Yes	Regarding 1.13, "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes". Our understanding of that criterion seemed clear until we read the rational and implementation reference document that states that "Control Systems that provide a "one-button push" capability of shedding 300 MW or more would also qualify as Critical Assets". That reference adds manual actuation with automatic therefore allowing additional interpretation of the meaning of the criterion. We also suggest replacing "capable of" with "purposed and programmed for" performing automatic load shedding of 300 MW or more within 15 minutes." A control system could be capable if programmed to do so but should not be included if that functionality is not its purpose.
Response: Thank you for your comments. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."		
Constellation Power Generation	Yes	Constellation Power Generation believes that in general, the criteria in Attachment #1 have drawn clear bright lines that will assist the industry in identifying critical assets. However, criterion 1.1, 1.5, and 1.11 need some further clarification and changes. Criterion 1.1 attempts to identify generation assets larger than 1500 MW. Constellation Power Generation (CPG) requests further clarification as to what constitutes a "single plant location." Would this include the aggregation of separated assets in separate structures with no shared resources other than being physically

Organization	Yes or No	Question 2 Comment
		located on a shared footprint? Constellation proposes the following changes to Criterion 1.1: Each group of generating units sharing a physical boundary with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. CPG also seeks clarification regarding the technical justification of the 1500 MW threshold. The SDT released a guidance document which did not fully explain the derivation of 1500 MWs. If this bright line was the average of reserve sharing in each of the 8 regions, than the value should be 1700 MWs, not 1500 MWs. CPG requests that the SDT reach out to the technical teams that exist within each region to obtain the correct reserve sharing thresholds. This data should be published, preferably in the guidance, to technically justify the seemingly arbitrary MW threshold. Criterion 1.5 attempts to identify cranking path equipment critical to a TOP's restoration plan. CPG is concerned that this criterion could be interpreted to include transformers and breakers associated with "the unit(s) being started." This implies that specific equipment at a generation asset may be critical while the asset itself may not be critical. This criterion would thus bring more equipment to scope that has little to no impact on the reliability of the BES. Constellation proposes the following changes to Criterion 1.5: 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the interconnection point of the generation asset to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. In addition, Item 1.11 should be removed from Attachment 1. Assets should not be deemed critical simply because they are associated with a nuclear facility. NRC regulations govern the safety and security of nuclear power plants. Rather, critical assets should be defined based upon reliability related criteria, independent of fuel type.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Organization	Yes or No	Question 2 Comment
Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets.		
Independent Electricity System Operator	Yes	We do not agree with criteria 1.6 and 1.7 as written since some of the facilities identified as Critical Assets by applying them may have no impact on the BES. We therefore believe the list of relevant transmission facilities developed by the Responsible Entity, should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. We therefore propose the following specific wording: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.
Response: Thank you for your comments. Items 1.6 and 1.7 – You propose to add the criteria that the RC can determine through a risk based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The inclusion of a risk-based evaluation by any entity would not meet the objective of uniform application of Critical Asset identification across all entities. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."		
American Electric Power (AEP)	No	AEP would contend that there are regional differences that would be relevant to determine a MW threshold for each responsible entity. We support the concept that was contained in the last draft that made the determination based on the capacity reserves. However, the prior language would need to be revisited to ensure that the value was fixed for a period of time. When do newly identified items in item 1.3. become in scope? During the annual review or does another review need to be done between annual reviews. Since many PA and TP are also Reliability Coordinators, Section 1.3 should be modified to contain "...required for long-term reliability purposes in the planning horizon." This should not include temporary seasonal reliability needs within the current year. Need a

Organization	Yes or No	Question 2 Comment
		requirement for the TP and PA to perform the analysis and have process for posting. Section 1.13 should be explicitly focused on BES elements and exclude distribution feeder interruptions. Would this include large industrial customers that can interrupt their loads? Net real power capability testing is defined in MOD-024 standards that have yet to be FERC approved. Furthermore, not all of the regions have defined the parameters for the capability testing. What would be the basis for defining the parameters for net real power capability determination? It is unclear in section 1.1 if what constitutes "single plant location." Is the physical location important or is it units that have common systems that could disrupt multiple units? AEP contents that it would not be logical to base the requirement on geographic address, but other factors such as voltage it is connect and the relationship of the units at the plant.
Response: Thank you for your comments. Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Item 1.3 – Newly identified Critical Assets come into scope at the time they are designated by the Planning Coordinator or Transmission Planner. Any associated newly identified Critical Cyber Assets would follow the "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities." This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.1 – CIP-002-4 does not require net real power capability testing. Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.		
Orlando Utilities Commission	Yes	SDT Proposed: 1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or

Organization	Yes or No	Question 2 Comment
		exceeding 1500 MW. OUC Comments: OUC believes that any system that has the ability to shed sufficient generation to cause system frequency to decline to the point of under-frequency relay protection tripping must be protected. OUC urges the drafting team to consider this aspect and re-design this requirement appropriately. This could probably be drafted as: "Any group of generating units at a single plant location that consist of more than 5% of the generation within a Balancing Authority" SDT Proposed: 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. OUC Comments: 1000MVAR is an arbitrary bright line suggest changing criteria to "Any reactive resource identified as a remedy, mitigation or strategy within a long range plan to address either real-time or contingency events. - or- Any reactive resource that if lost or destroyed while in service would result in a voltage change of more than 5% or a change in transmission loading that would result in an overload of a transmission element of more than 125% SDT Proposed: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. OUC Comments: Combine 1.4 and 1.5 path into single criteria to prevent expected interpretations and entity miss-understandings. In order to clearly identify "what's in and what's out" re-write the criteria as: "All facilities identified within a Transmission Operators restoration plan, required to establish a least one synchronized tie with a neighbor" The simplicity of this re-write is that it truly meets the requirements of rebuilding the BPS after an event. SDT Proposed: 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. OUC Comments: OUC believes that criteria 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations). SDT Proposed: 1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). SDT Proposed: 1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection

Organization	Yes or No	Question 2 Comment
		Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). SDT Proposed: 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. OUC Comments: OUC believes that any system that has the ability to shed sufficient load to cause frequency to increase to the point of over-frequency protection tripping must be protected, this includes system traditionally know as manual load shedding. OUC urges the drafting team to consider this aspect when re-designing this requirement. This could probably be drafted as: "Any system that can be configured to automatically drop 5% of load within a Balancing Authority based on either an automatic or manual initialization" SDT Proposed: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. OUC Comments: OUC understands the inter-connectedness of control centers and the risk even a small control center could pose to larger control centers, however this is the reason that strong security controls must exist for control centers that meeting the bright line criteria. However OUC is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15. OUC offers the following revised wording: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. SDT Proposed: 1.16. Any additional assets that the Responsible Entity deems appropriate to include. OUC Comments: OUC believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.
Orlando Utilities Commission	Yes	Question 2 Comments:

Organization	Yes or No	Question 2 Comment
		SDT Proposed: 1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. OUC Comments: OUC believes that any system that has the ability to shed sufficient generation to cause system frequency to decline to the point of under-frequency relay protection tripping must be protected. OUC urges the drafting team to consider this aspect and re-design this requirement appropriately. This could probably be drafted as: ”Any group of generating units at a single plant location that consist of more than 5% of the generation within a Balancing Authority” SDT Proposed: 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. OUC Comments: 1000MVAR is an arbitrary bright line suggest changing criteria to "Any reactive resource identified as a remedy, mitigation or strategy within a long range plan to address either real-time or contingency events. - or- Any reactive resource that if lost or destroyed while in service would result in a voltage change of more than 5% or a change in transmission loading that would result in an overload of a transmission element of more than 125% SDT Proposed: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. OUC Comments: Combine 1.4 and 1.5 path into single criteria to prevent expected interpretations and entity miss-understandings. In order to clearly identify "what’s in and what’s out" re-write the criteria as: "All facilities identified within a Transmission Operators restoration plan, required to establish a least one synchronized tie with a neighbor" The simplicity of this re-write is that it truly meets the requirements of rebuilding the BPS after an event. SDT Proposed: 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. OUC Comments: OUC believes that criteria 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations). SDT Proposed: 1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.8 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station).

Organization	Yes or No	Question 2 Comment
		SDT Proposed: 1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). SDT Proposed: 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. OUC Comments: OUC believes that any system that has the ability to shed sufficient load to cause frequency to increase to the point of over-frequency protection tripping must be protected, this includes system traditionally know as manual load shedding. OUC urges the drafting team to consider this aspect when re-designing this requirement. This could probably be drafted as: ”Any system that can be configured to automatically drop 5% of load within a Balancing Authority based on either an automatic or manual initialization” SDT Proposed: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. OUC Comments: OUC understands the inter-connectedness of control centers and the risk even a small control center could pose to larger control centers, however this is the reason that strong security controls must exist for control centers that meeting the bright line criteria. However OUC is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15. OUC offers the following revised wording: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. SDT Proposed: 1.16. Any additional assets that the Responsible Entity deems appropriate to include. OUC Comments: OUC believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Organization	Yes or No	Question 2 Comment
Orlando Utilities Commission	Yes	SDT Proposed:1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. OUC Comments:OUC believes that any system that has the ability to shed sufficient generation to cause system frequency to decline to the point of under-frequency relay protection tripping must be protected. OUC urges the drafting team to consider this aspect and re-design this requirement appropriately. This could probably be drafted as:"Any group of generating units at a single plant location that consist of more than 5% of the generation within a Balancing Authority" SDT Proposed:1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. OUC Comments: 1000MVAR is an arbitrary bright line suggest changing criteria to "Any reactive resource identified as a remedy, mitigation or strategy within a long range plan to address either real-time or contingency events. - or- Any reactive resource that if lost or destroyed while in service would result in a voltage change of more than 5% or a change in transmission loading that would result in an overload of a transmission element of more than 125% SDT Proposed:1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. OUC Comments:Combine 1.4 and 1.5 path into single criteria to prevent expected interpretations and entity miss-understandings. In order to clearly identify "what's in and what's out" re-write the criteria as: "All facilities identified within a Transmission Operators restoration plan, required to establish a least one synchronized tie with a neighbor" The simplicity of this re-write is that it truly meets the requirements of rebuilding the BPS after an event. SDT Proposed:1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. OUC Comments: OUC believes that criteria 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations). SDT Proposed:1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.8 should be reworded to "station or substation" instead of just

Organization	Yes or No	Question 2 Comment
		"station" so that it is not implied that it only applies to power plants (station). SDT Proposed:1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). OUC Comments: OUC believes that criteria 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). SDT Proposed:1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. OUC Comments: OUC believes that any system that has the ability to shed sufficient load to cause frequency to increase to the point of over-frequency protection tripping must be protected, this includes system traditionally know as manual load shedding. OUC urges the drafting team to consider this aspect when re-designing this requirement. This could probably be drafted as:"Any system that can be configured to automatically drop 5% of load within a Balancing Authority based on either an automatic or manual initialization" SDT Proposed:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. OUC Comments: OUC understands the inter-connectedness of control centers and the risk even a small control center could pose to larger control centers, however this is the reason that strong security controls must exist for control centers that meeting the bright line criteria. However OUC is concerned that criteria 1.14 is overly broad because it includes all BA and TOP control centers regardless of size. We understand the critical nature of control centers and the need to protect against loss of control of major sections of the BES. However, we ask that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15.OUC offers the following revised wording:1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. SDT Proposed:1.16. Any additional assets that the Responsible Entity deems appropriate to include. OUC Comments: OUC believes that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Item 1.2 – The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality. The SDT does not feel that a power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. Items 1.4 and 1.5 – NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. NERC standard EOP-005-2 R1.5 requires the Transmission Operator to identify Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started. The Facilities identified in compliance with this standard would be the Facilities classified as Critical Assets for Criteria 1.4 and 1.5. Criterion 1.5 has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.7 – The SDT agrees to change "stations" to "stations or substations." This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 –The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 - The SDT agrees to change "stations" to "stations or substations." This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		

Organization	Yes or No	Question 2 Comment
Oglethorpe Power Corporation	Yes	In general the criteria are very clear and concise and do not require additional explanations. It may however be appropriate, possibly in a separate document to provide some background on how these criteria were arrived at - especially criteria 1.1, 1.2 1.7, 1.13, and 1.15 which rely on seemingly arbitrary limits to determine the inclusion or exclusion of Assets. Additionally, some examples for criterion 1.16 may be a good idea.
Response: Thank you for your comments. Please refer to the draft guidance document posted on the Project 2008-06 page http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf		
Brazos Electric Power Cooperative, Inc.	Yes	In criterion 1.2 the use of the term "nameplate rating" should be replaced with "capability" and add "in the preceeding 12 months" at the end similar to criterion in 1.1. The use of the term "misused" in criterion 1.8, 1.9, 1.10 and 1.12 should be dropped as it leads to interpretation problems and doesn't improve reliability posture.
Response: Thank you for your comments. Item 1.2 – The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The term “misused” is in the criteria in response to FERC Order 706.		
Midwest ISO	No	Criteria 1.8, 1.9, and 1.12 should be modified because loss of facilities does not cause an IROL violation. An IROL includes a limit and a time constant Tv. In order for an IROL violation to occur, the limit must be exceeded for at least the time constant Tv. Tv is usually 30 minutes. Thus, when we consider the impact on the loss of facilities on an IROL, an operator will have enough time to adjust the system to prevent an IROL violation. For 1.8, the criterion should be modified to reflect that the facilities that comprise an IROL should be considered critical. The drafting team may also wish to consider loss of any facilities that set up the need for the IROL or cause the actual limit to change. For criterion 1.9, it is not clear why FACTs devices need to be singled out. Are they not covered in criterion 1.8 under Transmission Facilities? Inclusion of 1.9 is redundant and just causes confusion because it causes the reader to infer that the drafting team intended for them to be treated differently when in fact the criterion is the same as 1.8. For criterion 1.12, it would be more appropriate to assess the impact of an SPS, RAS, or automated switching system on the IROL. If loss of the SPS, RAS, or automated switching system causes an IROL to decrease, then the SPS, RAS, or automated switching system should be considered critical. Contrary to the companion

Organization	Yes or No	Question 2 Comment
		draft guidance document statement in the second paragraph on page 11, most SPS, RAS and automated switching systems are not used to prevent disturbances that would result in IROLs. In fact, some regions consider generation runback schemes to be an SPS even when it is used to simply resolve a generation outlet issue for loss of a line out of a plant. This is a common and economically effective way to avoid the expense of building more transmission lines. This paragraph from the draft guidance document should be removed. In the first bulleted paragraph on page 7 of the companion draft guidance document, the paragraph appears to conclude that a substation is a Facility. We disagree that it is facility. Because a facility is defined as a set of equipment that operates as a single BES Element and Element is further defined as "Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line." We believe facilities terminate in substations (i.e transmission line) or are wholly contained in a substation (i.e. transformer); however, we don't believe that a substation would fit the definition of facility as a result because it is not an electrical device with its own terminals that are connected to other electrical devices. The draft guidance document needs to be modified to reflect this. In the last paragraph on page 10 of the generation section draft guidance document, there is a discussion of Cranking Paths. Shouldn't this be moved to the transmission section?
Response: Thank you for your comments. Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – FACTS devices were singled out to ensure that there was no confusion as to whether or not they were considered Critical Assets. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." In the first bulleted paragraph on page 7 of the companion draft guidance document (posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf), the following is stated: "For example, for Transmission assets, the substation may be designated as the group of Facilities." Since the Cranking Path may contain both generation and Transmission Facilities, it is appropriate to discuss in both sections.		
Duke Energy	Yes	1.1 - Consistent with Criteria 1.8 and 1.9, this criterion should be conditioned by adding the phrase "unless planning studies are available to demonstrate that the loss of generation does not cause violation of one or more Interconnection Reliability Operating Limits (IROLs)." Related to the generation loss impact on Interconnection frequency and resource adequacy, Duke Energy disagrees with the arbitrary selection of the

Organization	Yes or No	Question 2 Comment
		generation loss MW amount for the following reasons: a) System inertia and frequency response factor into potential impact a generation loss could have on Interconnection frequency, and are different for each Interconnection. A 1,500 MW loss in the Eastern Interconnection is much less significant in terms of the initial frequency deviation than a similar loss within any other Interconnection. b) The limit fails to recognize the options available to the Balancing Authority to restore its balance within the existing criteria of the NERC reliability standards. For example, recovery from the loss of 1,500 MW within a 5,000 MW Balancing Authority may be quite different than recovery from a 1,500 MW loss within a 135,000 MW Balancing Authority in the Eastern Interconnection. PJM alone is about twice the size of ERCOT. 1.2 - We believe that 1000 MVAR may too large, and should be reduced to 500 MVAR. However criterion 1.2 could just be deleted, since any significant reactive resources would be picked up under criterion 1.8 1.3 - "Generation designated as required for reliability purposes" doesn't seem to be a very "bright line". We believe this criterion should be further clarified by including language from the "Rationale and Implementation Reference Document". 1.4 - Need to clarify that this criterion only includes the primary Blackstart Resources. Entities may include various alternative resources in their restoration plans which aren't Critical Assets, but which may not be clearly distinguished from the primary Blackstart Resources in the restoration plan. Add the phrase "that the entity intends to rely on for system restoration". 1.5 - The CIPDT is looking to the industry to define Critical Assets based on NERC definitions that are somewhat ambiguous and can be redefined by Standard Drafting Teams any time a group of standards is proposed. This could lead to Critical Assets being removed or added without proper analysis being performed on the impact to the system. Also, the definition of Cranking Path could be debated that it could be from a generating source that provides electricity to a larger resource during restoration. This source could be a small diesel that is sitting next to a large generator that provides the electricity to lift pumps, exciter field, or some other device that provides the means for a larger generator to become a Blackstart Resource. Or it could be argued that the cranking path is from a Blackstart Resource to fossil plants on the system that are used to facilitate the restoration of the system. Duke Energy requests that the Drafting team rewrite this requirement so that it does not use this term. Duke Energy also believes that the CIPDT should get input from those that are familiar with Restoration by requesting input from the Emergency Operations Drafting Team. We propose rewriting 1.5 as follows: The Facilities comprising the current carrying path from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point where multiple path options exist. 1.8 & 1.9 - These two criteria need clarification. First, it should be made clear that this IROL evaluation is to be made in the planning timeframe, because the purpose is to identify Critical Cyber Assets that need to be protected, which is an activity that takes place in the planning timeframe. Also, including the word "destroyed" in the phrase "destroyed, degraded, misused or otherwise rendered unavailable" creates significant

Organization	Yes or No	Question 2 Comment
		uncertainty regarding what the IROL analysis is intended to encompass. Add the phrase "via cyber attack" after the word "unavailable". This will clarify that the evaluation only encompasses destruction, degradation or misuse that can be achieved via cyber attack, and not a physical attack on the station. For example, physical attack could imply multiple transmission lines shorted to ground, which entails a much different analysis than transmission lines removed from service via cyber attack. NOTE: The physical security provided by the CIP standards is focused on protection of the Critical Cyber Assets, not the Critical Assets. 1.10 - As with our comment on 1.8 & 1.9 above, add the phrase "via cyber attack" after the word "unavailable". We also have a concern that if an entity fails to identify a facility under 1.1 or 1.3, they will also be in violation for failing to identify the corresponding Transmission Facilities under 1.10 (i.e. the double jeopardy issue). Need to replace the phrase "described in" with the phrase "identified by an entity pursuant to". Alternatively, 1.10 could be folded into 1.1 and 1.3 by adding the phrase "and Transmission Facilities providing the generation interconnection" to those criteria. 1.11 - Need to clarify that these Transmission Facilities are those that are specifically identified in the Nuclear Plant Interface Requirements (NPIRs) in the Agreement developed between the Nuclear Plant Generator Operator and applicable Transmission Entities pursuant to NUC-001-2. At the end of this criterion add the phrase "in the Agreement(s) required by NUC-001 R2." 1.12 - As with our comment on 1.8 & 1.9 above, this criterion should be revised to clarify that this IROL evaluation is to be made in the planning timeframe, because the purpose is to identify Critical Cyber Assets that need to be protected, which is an activity that takes place in the planning timeframe. Also, the phrase "destroyed, degraded, misused or otherwise rendered unavailable" needs to be clarified by adding the phrase "via cyber attack" after the word "unavailable". 1.13 - Load control programs shouldn't be defined as Critical Assets but rather Critical Cyber Assets, since they are a function of the control center, which is already a Critical Asset. Replace the word "Common" with the phrase "Each control center or backup control center used to". Also, clarify the meaning of "automatic" by inserting the parenthetical (without human intervention) after the word "automatic". 1.14 - This criterion is far too broad because we don't have an approved NERC definition of control room, control system, backup control room or backup control system. Many switchyards and substations have control systems that could be used to perform transmission functions, but that doesn't mean that they are "Critical Assets". Remove control system and backup control system from this criterion and limit it to identifying the control centers and backup control centers associated with the Critical Assets on the transmission system, just as criteria 1.15 links identification of the control center or backup control center to the generation asset. We propose rewriting 1.14 as follows: Each control center or backup control center associated with the Critical Assets on the transmission system. 1.16 - A "catch-all" criterion seems inappropriate in a "bright line" list. You can always go beyond the

Organization	Yes or No	Question 2 Comment
		requirements of a standard and do more than what's required.

Response: Thank you for your comments.

Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities.

Item 1.2 – The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.5 – NERC standard EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" designates that Cranking Paths must be identified. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Items 1.8 & 1.9 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets. Criterion 1.8 has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.9 has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.10 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets. There is no double jeopardy, since all of these criteria are contained in the same Requirement. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."

Item 1.11 – The SDT does not believe that adding the phrase "in the Agreement(s) required by NUC-001 R2" provides any clarification, since the defined NERC term Nuclear Plant Interface Requirements is "The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by

Organization	Yes or No	Question 2 Comment
the Nuclear Plant Generator Operator and the applicable Transmission Entities." Item 1.12 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets. This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.		
Seminole Electric Cooperative, Inc.	Yes	1. A general comment is that there is no technical justification provided for the proposed criteria. The "Rationale and Implementation Reference Document" does not provide technical justification, but rather provides more of an opinion of the drafting team. To the extent possible, there should be technical justification for the proposed criteria that stakeholders can review. 2. SEC is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). SEC understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator's restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a Critical Asset.To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a

Organization	Yes or No	Question 2 Comment
		10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, SEC would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. 3. In item 1.7 the statement regarding "three or more other transmission stations" is confusing. A better explanation is needed -- does this mean stations upstream, downstream, networked or radial? 4. In item 1.14 the term "control center" must be defined, especially when dealing with the significance of the requirements of this standard. Using an undefined term here is inappropriate. 5. In item 1.14 its states that all RC, BA and TOP control centers, etc., are Critical Assets. While SEC agrees with this as it relates to RCs, we do not agree with this as it relates to all BAs and TOPs. In the draft CIP-010 there was high, medium and low criteria which in many instances appropriately matching CIP requirements to the level of risk certain assets potentially present to the BPS. SEC strongly believes that the CIP-002-4 standard requirements for smaller BAs and TOPs should match the lower level of risk to BPS reliability that these smaller BAs and TOPs potentially present. Similar to the 1500MW size criteria that is included in item 1.15 for generator control centers, there should be size criteria for the smaller BAs and TOPs. The drafting team should modify item 1.14 to state that all control centers with a peak demand above 2000MW (same as medium criteria in draft CIP-010) shall be designated as a Critical Asset. This is the lowest SEC could support and also recommend its members to support. We firmly believe that this would capture all of the control centers that truly have a material impact on the reliability of the BPS. 6. Related to the Critical Asset Criteria, there should be a provision in the standard that provides a process for an entity to technically demonstrate that even though the criteria identifies some of their assets as Critical Assets, their assets (or a portion thereof) do not meet the definition of a Critical Asset and should be excluded from applicability of CIP-003 through CIP-009.

Response: Thank you for your comments.

The SDT believes information provided in the guidance document (posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf) provides sufficient technical justification for each criterion.

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT believes that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Organization	Yes or No	Question 2 Comment
Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation-only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. This criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.14 - At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.		
Progress Energy	Yes	General Comments:The terms "degraded" and "misused" are subject to a wide range of interpretation, are not auditable and should not be used in bright line standards. Measurable values should be provided. Criterion 1.1: What is meant by "at a single plant location" should be clarified. Generating units that constitute a plant should be defined based on electrical connection. Criterion 1.5: Clarification is needed on what is included beyond blackstart generation units. Criterion 1.8: This requirement should be set aside from this version of the standard and be re-introduced in the next version with appropriate measureable parameters for High, Medium and Low Impact BES facilities. Criterion 1.9: Same comments as for Criterion 1.8. Criterion 1.11: The criteria should be: The local nuclear plant switchyards, the transmission lines connected to these switchyards, and the first out substations on the other ends of these transmission lines. These are the transmission facilities essential to meeting the NPIRs. Criterion 1.13: Distribution should be specifically excluded from this criterion because loss of distribution facilities does not affect the BES.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments. The terms "degraded" and "misused" are in the criteria in response to FERC Order 706. Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. The document is posted on the Project 2008-06 page at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant. Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5 "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started" where the Transmission Operator can choose between the next Facilities on the BES to energize. This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.8 and Item 1.9 – Criteria 1.8 and 1.9 include those Transmission Facilities that would violate IROLs if they were rendered unavailable or degraded. By definition, IROLs are those operating limits that, if exceeded, would have a Wide Area reliability impact. Criterion 1.8 has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Criterion 1.9 has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."		
New York Independent System Operator	Yes	The NYISO request that the NERC Glossary include definitions for all terms especially in Attachment 1. Examples to add to the NERC Glossary or the standard would be to define: control center, control system, backup control center, and backup control system
Response: Thank you for your comments. At this time, the SDT is choosing not to add terms to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.		
Cowlitz County PUD	Yes	Further 'red line' criteria needs to be added to avoid inclusion of non-critical assets.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comments.		
Kansas City Power & Light	No	Absent engineering analysis and study, this bright line proposal does not establish a sound basis for capturing the elements that should be included and those that should be excluded. Very concerned regarding the proposed criteria specified by criteria 1.4, 1.5, 1.13 and 1.14 as this criteria will identify assets as critical assets for smaller entities that have no regional reliability impact on the bulk electric system and will place an unnecessary compliance burden on them. These criteria need to either be considered for removal or modification such that an applicable application is achieved.
Response: Thank you for your comments. The SDT does not feel that engineering analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact the results of the analysis. Such studies would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions.		

3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: The majority of commenters that disagreed with Requirement R1 suggested changes to wording that is present in the existing CIP-002-3. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology mentioned exists in the existing CIP-002-3 standard. The SDT expects the phraseology to be resolved in the next version. Others stated that their objection was with the wording in Attachment 1. The SDT directed them to the responses offered to their comments in question 2.

Organization	Yes or No	Question 3 Comment
Northeast Power Coordinating Council	Disagree	Request an explicit definition of "annual." Because the "update as necessary" in R1 is not clear, the new assets effective date is in doubt. Should be it be part of "update as necessary" or part of the annual review? The standard clearly mentions the documentation required to comply with CIP-002-4. This includes - list of Critical Assets as specified in R1, list of Critical Cyber Assets as specified in R2, and approval records of annual approvals as specified in R3. However, in the Guidance document, Page 7, bullet point 2, second sentence, it states the following - "...Responsible Entity should document all criteria that qualify this asset as a Critical Asset..." The drafting team should clarify documentation requirements to avoid discrepancies. If it is expected that entities are to document, and retain documentation, of the criteria that supports the categorization of critical assets, this should be explicitly required by the standard. As the proposed standard is written, the only documentation registered entities must create and retain is the actual list of the assets.Agreement based on the assumption that the classifications in Attachment 1 are corrected.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. The standard specifies the requirements that the Responsible Entity must comply with. The reference document is intended to provide guidance and does not specify any requirement for compliance.		
City of Garland	Agree	

Organization	Yes or No	Question 3 Comment
NRG Energy Inc.	Agree	
APPA CIP-002-4 Task Force	Agree	
IRC Standards Review Committee	Agree	The SRC agrees with the obligations prescribed by R1, subject to the SDT's acceptance of the proposed revisions described in response to Question 1.
Response: Thank you for your comments.		
Bonneville Power Administration	Agree	We agree with the "at least annually" aspect of the requirement. Annual review seems appropriate if a utility has not had any major changes or expansion to their grid since their last Critical Asset determination.
Response: Thank you for your comments.		
PSEG Companies	Agree	
Pepco Holdings, Inc - Affiliates	Agree	Requirement 3 should be modified: References to risk-based assessment methodology should be removed.
Response: Thank you for your comments. This requirement will modified prior to the next ballot.		
MRO's NERC Standards Review Subcommittee	Agree	We agree with the annual application of the criteria, however, we want to be clear that we do not agree with all of the criteria listed in Attachment 1. We have included suggested improvements to the criteria under question #2.For clarity, we suggest that the final sentence of this requirement be reworded as follows:"The Responsible Entity shall review this list at least annually, and update it as necessary based on the findings of this review."
Response: Thank you for your comments.		
Santee Cooper	Disagree	We would agree with requirement R1 if Attachment 1 is refined to be more reasonable.
Response: Thank you for your comments.		
Dominion	Agree	

Organization	Yes or No	Question 3 Comment
Edison Mission Marketing and Trading	Agree	
Florida Municipal Power Agency	Disagree	FMPA recommends avoiding the use of the term "Annual" due to the ambiguity of the term. Instead something like once a calendar year but no longer than 15 months may be more appropriate.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.		
PNGC Power	Disagree	Please see criteria in answer to question #2. We do agree with annual review requirement.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.		
WECC	Agree	
Southern Company	Agree	
Encari, LLC	Disagree	The Guidance document states a Critical Asset should be listed by only one Responsible Entity. We therefore question why Generator Operators and Transmission Operators are included as Responsible Entities subject to Requirement R1 of draft CIP-002-4
Response: Thank you for your comments. Generator Operators and Transmission Operators are listed as possible Responsible Entities to address cases where there may be a formal agreement for these Entity types to be responsible for compliance to the CIP requirements: In addition, control centers are typically owned by Generator Operators and Transmission Operators. We have modified the guidance document to reflect this.		
Arizona Public Service	Agree	
Edison Electric Institute	Agree	
Tennessee Valley Authority (TVA)	Agree	None.

Organization	Yes or No	Question 3 Comment
PacifiCorp	Agree	
OGE	Agree	
FMPA	Disagree	FMPA recommends avoiding the use of the term “Annual” due to the ambiguity of the term. Instead something like once a calendar year but no longer than 15 months may be more appropriate.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
South Carolina Electric and Gas	Agree	
Pinellas County Resource Recovery Facility	Agree	
Central Lincoln	Agree	
Edison Mission Marketing and Trading	Disagree	The same question for this one. CIP-002-4 Attachment 1-1.1 what is the basis for the 1500 MW versus what used to be Output exceeds Reserve Sharing Group obligation or Output exceeds Contingency Reserve obligation
Response: Thank you for your comments. Please refer to the response to your comment in Question 2.		
SPS Consulting Group Inc.	Disagree	While I agree with the development of a list and the annual application of the criteria, the "update as necessary" phrase is ambiguous. This is the kind of language that has led to multiple interpretation requests and should never be in a reliability standard requirement. Suggest deleting "and update it as necessary." Annual review should be sufficient to insure protection.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Tacoma Power	Agree	Tacoma Power agrees with the SDT using a defined list for identifying Critical Assets. However, Tacoma Power recommends that the SDT make the recommended changes noted in Question 2

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comments.		
Green Country Energy	Agree	
Illinois Municipal Electric Agency	Agree	
Minnkota Power Cooperative	Agree	
Horizon Wind Energy	Agree	Agree with the annual application of the criteria, but provided comments below on the actuall criteria used.Criteria 1.15 in attachments A includes generation control centers used to control generation greater than an aggregate of 1500 MWs in a single interconnection. It is true that the span of control of the generation control center may cross multiple BA or RSG areas. In the unlikely event of a common mode failure of such a generation control center that would lead to a loss of all generation, the loss of generation in the multiple BAs or RSGs could fall significantly below the criteria of the 1500 MWs threshold used in criteria 1.1 for generating units at a single plant location, therefore not affecting the reliability and operability of the BES system. There seems to be a disconnect in criteria 1.1 for generation and 1.15 for generation control centers, hence 1500 MWs in a single plant location vs. 1500 MWs aggregate in a single interconnection for generation control centers. Secondly, some generation control centers collect data from generators via SCADA for monitoring purposes and can manually send set points to lower generation if the need would arise. Does this type of arrangement fall under the description of control generation or was it the intent to include, in the description, generation that is controlled to maintain sufficient Contingency Reserve (BAL - 002) and Resource and Demand Balancing (BAL - 003)? Suggest adding language to 1.15 that is more in line with the criteria in 1.1 and clarifying what is meant by control generation.
Response: Thank you for your comments. Please refer to the response to your comment in Question 2.		
Union Power Partners LP	Agree	With consideration of the responses to questions 1 & 2.
Response: Thank you for your comments.		
MidAmerican Energy Company	Agree	
North Carolina Membership Corporation	Disagree	Because NCEMC does not currently agree with all of the provisions in Attachment 1 - Critical Asset Criteria, we cannot at this time agree with this question.

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comments.		
Hydro One Networks Inc.	Agree	
Dynegy Inc.	Agree	
Matrikon Inc.	Agree	
Northeast Utilities	Agree	
CenterPoint Energy	Agree	CenterPoint Energy has no concerns with the verbiage in Requirement R1 but, as noted in our previous comments, CenterPoint Energy recommends deletion of proposed Criteria 1.11 in Attachment 1.
Response: Thank you for your comments.		
LCEC	Agree	Agree with the concept but not the criteria. See response to questions 1 & 2.
Response: Thank you for your comments.		
Xcel Energy		
Great River Energy	Disagree	Does not allow for individual interpretation and application
Response: Thank you for your comments. The changes to CIP-002-4 specifically address issues of uniform application across all entities.		
ITC Holdings	Agree	
Public Utility District No. 1 of Clark County	Agree	This is a reasonable expectation of Responsible Entities.
Response: Thank you for your comments.		
TransAlta		

Organization	Yes or No	Question 3 Comment
Exelon	Disagree	If as expected the NRC accepts the exception process proposed by NERC as part of resolving the Bright-Line Survey, regulation of BOP cyber assets will be by NRC. However, FERC Order 706B remains in force, resulting in the need for Nuclear GO/GOP entities to comply with CIP-002 and annually determine CAs, and then reiterate to NERC that all BOP cyber assets are regulated by NRC. Nuclear makes the comment that with NRC regulation of BOP cyber assets, the annual CIP-002-4 R1 CA determination is unnecessary and we recommend that Nuclear GO/GOP again be exempted from each of the NERC CIP Reliability Standards CIP-002 thru -009.
Response: Thank you for your comments. The proposed standards are drafted with the current regulatory regime in effect and cannot be drafted on any speculation on future outcomes in this area.		
AECI	Agree	
N.W. Electric Power Cooperative, Inc.	Agree	
Central Electric Power Cooperative	Agree	
Central Electric Power Cooperative	Agree	
M & A Electric Power Cooperative	Agree	
LCRA Transmission Services Corporation	Agree	
Sho-Me Power Electric Cooperative	Agree	
KAMO Power	Agree	
United Illumiinating	Agree	

Organization	Yes or No	Question 3 Comment
Constellation Energy Commodities Group	Agree	
Associated Electric Cooperative, Inc.	Agree	
KAMO Electric Cooperative	Agree	
Northeast Missouri Electric Power Cooperative	Agree	
NW Electric Power Cooperative, Inc.	Agree	
Sierra Pacific Power d/b/a NV Energy	Agree	
Sho-Me Power Electric Cooperative	Agree	
SDG&E	Agree	SDG&E generally agrees with R1 given the comments outlined in question #2 above are incorporated
Response: Thank you for your comments.		
Central Lincoln	Disagree	Central Lincoln believes that "annually" should be further clarified. It could be interpreted to either be once in a calendar year or once every twelve months. If the later is intended, suggest specifying a maximum interval to allow for review dates that could otherwise fall on weekends, holidays, or during emergencies. We suggest a maximum interval of 15 months. It remains unclear how assets that are newly discovered to be critical during these reviews are to be treated, as discussed below.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Northeast Missouri Electric	Agree	

Organization	Yes or No	Question 3 Comment
Power Cooperative		
National Rural Electric Cooperative Association (NRECA)	Disagree	Since NRECA disagrees with the current CIP-002-4 Attahcment 1 -- Critical Asset Criteria document, we could not select "Agree" here. If requested modifications are made to Attachment 1, then we could agree with R1.
Response: Thank you for your comments.		
Tampa Electric	Agree	
M&A Electric Power Cooperative	Agree	
MEAG Power	Agree	
Associated Electric Cooperative, Inc.	Agree	
Associated Electric Cooperative, Inc.	Agree	
FirstEnergy Corp	Agree	
Minnesota Power	Agree	
Manitoba Hydro	Agree	
American Transmission Company	Agree	
Ameren	Disagree	We would agree to review the critical asset list as least annually but we do not agree with the bright line criteria in Attachment 1, see comments for question 2.
Response: Thank you for your comments. Please refer to response to comment in question 2.		
BGE	Agree	Pending the suggested changes to the Attachment 1 and clarify wording as follows: “Critical Asset

Organization	Yes or No	Question 3 Comment
		Identification - Each Responsible Entity shall develop a list of its Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria. The Responsible Entity shall review its Assets at least annually by applying the criteria contained in CIP-002-4 Attachment 1 Critical Asset Criteria, and update the Critical Asset list as necessary."
Response: Thank you for your comments. There is not a compelling reason offered to remove the word "identified" from R1. Additionally, the word is in the previous three versions.		
Beaches Energy Services (of City of Jacksonville Beach, FL)	Disagree	We recommend avoiding the use of the term "Annual" due to the ambiguity of the term. Instead something like "Once a calendar year, but no longer than 15 months" may be more appropriate.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
We Energies	Agree	
City Utilities of Springfield, MO	Agree	SPRM agrees with the proposed Requirement.
Response: Thank you for your comments.		
National Grid	Agree	The standard clearly mentions the documentation required to comply with CIP-002-4 which includes - list of Critical Assets as specified in R1, list of Critical Cyber Assets as specified in R2, and approval records of annual approvals as specified in R3. However, in the Guidance document, Page 7, bullet point 2, second sentence, it states the following - "...Responsible Entity should document all criteria that qualify this asset as a Critical Asset..." National Grid recommends that the drafting team clarifies the documentation requirements to avoid such discrepancies. If the standards drafting board expects entities to document, and retain documentation, of the criteria that supports the categorization of critical assets, this should be explicitly required by the standard. As the proposed standard is written, the only documentation registered entities must create and retain is the actual list of the assets.
Response: Thank you for your comments. The standard specifies the requirements that the Responsible Entity must comply with. The reference document is intended to provide guidance and does not specify any requirement for compliance.		
Lincoln Electric System	Agree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comments.		
Southwest Power Pool Regional Entity	Disagree	Clarify that the first application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria and the associated identification of Critical Assets must take place on or before the effective date of the approved standard. This affords the entity a minimum of six months to complete the required assessment. (The auditors will seek evidence based on this expectation, so placing it in the standard or accompanying guidance will remove any ambiguity such as that experienced with Version 1 of the standards)
Response: Thank you for your comments. The implementation plan (posted on the Project 2008-06 project page at http://www.nerc.com/docs/standards/sar/Project2008-06_Implementation_Plan_CIP_V4Standards.pdf) specifies the proposed compliance schedule of the standards and requirements.		
Indianapolis Power & Light	Agree	
Constellation Power Generation	Agree	
Independent Electricity System Operator	Disagree	While we don't disagree with Requirement R1 per se, we do have concerns about criteria 1.6 and 1.7. (See our response to Question 2 which includes a suggestion for a new requirement to be placed on the Reliability Coordinator.) Also, we do not agree with the removal from the Applicability Section, of the exclusion that applies to facilities regulated by the Canadian Nuclear Safety Commission. This explicit statement makes it clear that CIP standards do not apply to those facilities which would not be the case if it were removed.
Response: Thank you for your comments. The applicability section has been modified to address the current Canadian regulatory issue for nuclear facilities. Please see response to question 2.		
American Electric Power (AEP)	Agree	AEP suggests that parts of requirement 3 could be added to requirements 1 and 2 and then Requirement 3 could be removed.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.		
Orlando Utilities Commission	Agree	
Oglethorpe Power Corporation	Disagree	An annual review of the CA and CCA lists is consistent with previous versions of the standards and in general this is a reasonable time frame for verifying that unplanned changes or changes outside the immediate

Organization	Yes or No	Question 3 Comment
		visibility of a given Registered Entity have not affected the status of the CA and/or CCA lists. However as the implementation plan points out, there are many changes (both corporate and technical) which are planned and for which entities should not wait for an annual review to determine whether they affect the entities' CA and CCA lists. The requirement should contain a reference to the implementation plan to ensure that such changes are made in a manner that maintains compliance throughout.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Brazos Electric Power Cooperative, Inc.	Disagree	The proposed requirement needs to clarify what "update it as necessary" means.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Midwest ISO	Agree	
Duke Energy	Disagree	Requirement R1 is acceptable except for the issues we've identified with Attachment 1 in our response to Question #2 above.
Response: Thank you for your comments. Please refer to response to question 2.		
Seminole Electric Cooperative, Inc.	Disagree	Must disagree based prior comments and disagreement with Attachment 1
Response: Thank you for your comments. Please refer to response to question 2.		
Progress Energy	Disagree	The term "annual" should be defined directly in the requirement. Alternatively, "annual application" could be replaced with "application of the criteria once every 12 months..." and "at least annually" could be replaced with "at least once every 12 months..." if that was the intention.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.		

Organization	Yes or No	Question 3 Comment
The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Orlando Utilities Commission	Agree	
New York Independent System Operator	Agree	The NYISO requests that the SDT be specific with respect to annual. The drafting team should consider using the phrase once every calendar year, or once every 15 months.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
Cowlitz County PUD	Agree	
Orlando Utilities Commission	Agree	
Kansas City Power & Light	Disagree	Do not disagree with annual review and updates for determination and identification of critical assets. The current bright line proposal lacks engineering and reliability assessment basis and is arbitrarily chosen to achieve a predetermined number of critical assets that may appear as valid, but in fact, may be lacking or too strong.
Response: Thank you for your comments. Regarding the need for additional engineering studies, the SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. The industry provided significant feedback for the need to simplify the Critical Asset identification approach. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. NERC issued a data request in August of 2010 to assist the SDT in developing a consistent approach to Critical Asset identification. The results of this request were used to assist the team in developing the criteria in Attachment 1.		

4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration: Of commenters that disagreed with Requirement R2, the majority suggested changes to wording that is present in the existing CIP-002-3. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology mentioned exists in the existing CIP-002-3 standard. The SDT expects the phraseology to be resolved in the next version. Some commenters had questions about the 15 minute qualifier. The SDT's response is that this phrase is inserted to limit the scope to "real time" operations, which is not a NERC defined term. Several commenters had suggested wording to clarify the requirement. Based on the comments received, Requirement R2 has been reworded to:

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Organization	Yes or No	Question 4 Comment
Northeast Power Coordinating Council	Disagree	In Attachment 1, Criterion 1.1, why is nuclear generation specifically mentioned? Does this have any implications for other fuel types? Refer to the response above for Question 3. If the intent is for entities to retain documentation of the basis for categorization, this should be explicitly stated in the standard. Otherwise the only documentation retained may be the list of assets. As noted in paragraph 236 of FERC Order 706, the proposed standard does not provide guidance on more accurate determination of critical cyber assets. The language regarding generation units adds confusion to the requirement for entities that are not involved in generation. It should be moved elsewhere such as a footnote or end note. The 15 minute criteria listed in R2 needs to be better described to avoid misinterpretation.
Response: Thank you for your comments. The phrase concerning nuclear generation does not change the scope. It is there to add clarification. Please see our response to Question 3. Please refer to the reference document (posted at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf) for guidance on documentation. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The language for generation units is necessary for determining the appropriate Critical Cyber Assets at generating plants and qualifies the immediately preceding requirement to identify Critical Cyber Assets. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impacts.		
City of Garland	Agree	
NRG Energy Inc.	Disagree	Need Clarification on routable path, discrete links and serial connections as it pertains to CIP-002-3 R3: Is a device considered to communicate outside the ESP using routable protocol if ANY portion of the communications path uses routable protocol? Need clarification concerning shared assets. Does it mean shared between a single device or same device on a network? R2 states that only shared cyber assets for a group of generating units at a single location identified in Attachment 1 criteria 1.1, namely the 1500 MWs brightline, that could impact reliable operation should be considered. Does this cyber asset identification only include assets meeting criteria 1.1 and

Organization	Yes or No	Question 4 Comment
		therefore exclude any cyber assets utilized for reliable operation of a designated critical asset such as a single blackstart resource? Please provide clarification in this requirement.
Response: Thank you for your comments. A response to the question regarding routable protocols depends on which part of the communication path you refer to. The guideline on identifying critical cyber assets provides an interpretation on various scenarios that might fit the case mentioned. The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1.		
APPA CIP-002-4 Task Force	Agree	
IRC Standards Review Committee	Disagree	See comments to Question 1 above and proposed Attachment 1.
Response: Thank you for your comments.		
Bonneville Power Administration	Disagree	The requirement as written continues and does not solve the ambiguity with the current Critical Cyber Asset identification requirement. Specifically: “essential to the operation of the Critical Asset” needs to be defined; “adversely impact the reliable operation” needs to be defined; and, it is not clear what “within 15 minutes” means in this context. The intent of the Standards Drafting Team needs to be made clear.
Response: Thank you for your comments. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The subjectivity involved in the Critical Cyber Asset identification requirement will be addressed in future releases of these Standards. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
PSEG Companies	Agree	
Pepco Holdings, Inc - Affiliates	Agree	
MRO's NERC Standards Review	Agree	For clarity, we suggest this requirement be reworded as follows:For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets

Organization	Yes or No	Question 4 Comment
Subcommittee		that must be considered are those shared Cyber Assets that could within 15 minutes adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1.
Response: Thank you for your comments. Requirement R2 has been changed to reflect your suggested wording.		
Santee Cooper	Disagree	We believe R2 is confusing as written, and detracts from the “bright line” concept. Specifically, the 15 minutes is confusing and is not explained well in the CIP-002-4 -Cyber Security- Critical Cyber Asset Identification Rationale and Implementation Reference Document. Perhaps the “within 15 minutes” could be reworded in this manner: Those shared assets which are inoperable for 15 minutes or more, which could cause loss of large generation amounts, will have to be considered. Those shared assets which are inoperable for 15 minutes or more, and could be restored within a reasonable amount of time, and do not cause loss of large generation amounts, would not have to be considered.
Response: Thank you for your comments. Requirement R2 has been changed to clarify the issues presented.		
Dominion	Disagree	While Dominion agrees conceptually with the SDT, we believe that the language in R2 could be improved if the following revision was made; "Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units identified as critical pursuant to Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of those units that in aggregate exceeds Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:”Additionally Dominion would like clarification of the 15 minute criteria. Does it apply to all cyber assets or just to the criteria of 1.1 and 1.13?
Response: Thank you for your comments. Requirement R2 has been changed to clarify the issues presented. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
Edison Mission Marketing and Trading	Agree	"... within 15 minutes." What exactly has to happen within 15 minutes?
Response: Thank you for your comments. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time		

Organization	Yes or No	Question 4 Comment
reliability impact.		
Florida Municipal Power Agency	Disagree	FMPA believes that a similar "shared Cyber Assets" criterion needs to be applied at a substation for transmission Facilities emanating from that substation in a similar fashion as is described for power plants. For instance, if the entire substation is found to be a Critical Asset as a result of application of Attachment 1, a single microprocessor based relay isolated and only operating one non-critical transmission Facility should not be swept into the standards. Instead, only shared Cyber Assets controlling the entire critical substation should be a Critical Cyber Asset. FMPA recommends avoiding the use of the term "Annual" due to the ambiguity of the term. Instead something like once a calendar year but no longer than 15 months may be more appropriate.
Response: Thank you for your comments. The term Transmission Facilities can be applied to either the entire substation or each Facility or group of Facilities connected to that substation, as determined by the entity. This would allow an entity which has multiple voltage levels at a single substation to either declare the entire substation as a Critical Asset or only the portion of the substation that qualifies under any particular criterion. The shared cyber asset qualifier only applies to criterion 1.1 because it refers to a group of generating units. The phraseology you are concerned about (annual) exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
PNGC Power		
WECC		The requirement as written does not resolve the ambiguity with the current Critical Cyber Asset identification requirement. Specifically: "essential to the operation of the Critical Asset" needs to be defined; "adversely impact the reliable operation" needs to be defined. It is also unclear what "adversly impact the reliabile operation of any combination of units within 15 minutes means. Is this intended to mean that anything that could adversly impact these same units in 20 minutes is not a threat or that it could be protected by operator intervention?
Response: Thank you for your comments. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The subjectivity involved in the Critical Cyber Asset identification requirement will be addressed in future releases of these Standards. The 15		

Organization	Yes or No	Question 4 Comment
minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
Southern Company	Agree	However, Southern recommends the following change, because this provision should not be limited to only criterion 1.1:"For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1,". In addition, the SDT should remove all references to "risk-based assessment" in R3, as this is no longer a Requirement under CIP-002-4 (this term was only partially removed from the revised 10-20-10 version). Importantly, the SDT should also add a provision which specifically excludes any Cyber Assets regulated by Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission. There is currently no reference to this exclusion in CIP-002-4.
Response: Thank you for your comments. The shared cyber asset qualifier only applies to criterion 1.1 because it refers to a group of generating units. The glossary definition for Transmission Facilities allows flexibility for defining the Critical Asset as one that operates as a single BES Element, in which case the relay operating a non-critical Transmission Facility would not be a CCA. All references to "risk-based assessment" will be removed prior to the next ballot. The Applicability section has been revised to address nuclear plants.		
Encari, LLC	Agree	
Arizona Public Service	Agree	
Edison Electric Institute	Agree	
Tennessee Valley Authority (TVA)	Agree	None.
PacifiCorp	Agree	
OGE	Agree	
FMPA	Disagree	FMPA believes that a similar "shared Cyber Assets" criterion needs to be applied at a substation for transmission Facilities emanating from that substation in a similar fashion as is described for power plants. For instance, if the entire substation is found to be a Critical Asset as a result of application of Attachment 1, a single microprocessor based relay isolated and only operating one non-critical transmission Facility should not be swept into the standards. Instead, only shared Cyber Assets controlling the entire critical substation should be a Critical Cyber Asset.FMPA recommends avoiding the use of the term "Annual" due to the ambiguity of the term. Instead something like once a calendar year but no longer than 15 months may be

Organization	Yes or No	Question 4 Comment
		more appropriate.
Response: Thank you for your comments. The term Transmission Facilities can be applied to either the entire substation or each Facility or group of Facilities connected to that substation, as determined by the entity. This would allow an entity which has multiple voltage levels at a single substation to either declare the entire substation as a Critical Asset or only the portion of the substation that qualifies under any particular criterion. The shared cyber asset qualifier only applies to criterion 1.1 because it refers to a group of generating units. The phraseology you are concerned about (annual) is in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.		
South Carolina Electric and Gas	Agree	
Pinellas County Resource Recovery Facility	Agree	I agree with the first and third sentences as written. I think the language in the second sentence is unclear. I agree with what I think it is saying! For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes.
Response: Thank you for your comments.		
Central Lincoln	Agree	
Edison Mission Marketing and Trading	Agree	
SPS Consulting Group Inc.	Disagree	See previous Question 3 concern about "as necessary" language. Also, I do not understand the reference to "within 15 minutes" in this requirement. Within 15 minutes of what? Of discovering a cyber intrusion? Of the inception of an actual breach of electronic security? Of a SCADA or EMS system (for example) being taken over by a hacker? This reference to 15 minutes also implies a time-stamped piece of evidence that would be extremely difficult to audit. One should put on their auditor hat and imagine sitting down with a Registered Entity and trying to verify compliance with this requirement. We need to do a better job of drafting requirements that are clear and do not put the auditors in the position of making ad hoc interpretations in order to complete the audit.

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comments. The 15 minutes limiter refers to the reliability impact and not the inception of a breach. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact. The SDT believes the Responsible Entity can provide evidence demonstrating how certain systems in a generating plant will not have a reliability impact within 15 minutes.		
Tacoma Power	Disagree	Tacoma Power Commends the SDT for recognizing that not all cyber assets within a generation facility are necessarily critical. The wording of the requirement however creates ambiguities. Tacoma Power feels that the statement, “For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes, “needs clarification. Tacoma Power suggests that the statement read, “For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes.”
Response: Thank you for your comments. Requirement R2 has been changed to clarify the issues presented.		
Green Country Energy	Agree	
Illinois Municipal Electric Agency	Agree	
Minnkota Power Cooperative	Agree	
Horizon Wind Energy	Agree	
Union Power Partners LP	Disagree	Would change the language to "those shared Cyber Assets accessible from outside malicious cyber intrusion that could adversely" in line 4.
Response: Thank you for your comment. The susceptibility of a Cyber Asset to malicious cyber intrusion is dependent on several factors, many of which are dynamic or		

Organization	Yes or No	Question 4 Comment
unknown, including the configuration of the Cyber Asset, the capability of the malicious threat and internal access. The set of CIP cyber security standards (CIP-002 to CIP-009) is a holistic approach to cyber security protection that applies to both internal and external threats.		
MidAmerican Energy Company	Agree	
North Carolina Membership Corporation	Disagree	Just as in question 3 NCEMC does not currently agree with all of the provisions in Attachment 1 - Critical Asset Criteria, we cannot at this time agree with this question.
Response: Thank you for your comment. Please refer to response to question 3 and question 2.		
Hydro One Networks Inc.	Disagree	
Dynegy Inc.	Disagree	For R2, it could be fine but needs further "specific" guidance on the Cyber Assets that could adversely.....impact....within 15 minutes". Suggest providing specific examples. For R3, remove the comment related to risk-based assessment methodology from the draft Standard.
Response: Thank you for your comment. Please refer to the guidance document posted at http://www.nerc.com/docs/standards/sar/Project_2008-06_CIP-002-4_Guidance_clean.pdf . References to the risk-based assessment will be removed prior to the next ballot.		
Matrikon Inc.	Disagree	I believe the original intent, yet never clearly documented, is that the "tampering and misuse" of cyber assets is also criteria to determine the relationship between the Critical Asset and its Cyber Assets. Is tampering and misuse the intent of this requirement? If so, it must be specifically stated, including a definition and direct statements if Entities are expected to use this criterion for identification of CCAs. Secondly, the 15 minute criterion is going to attract alot of attention and interpretation, further guidance is recommended in the form of scenarios, events and examples. Otherwise, inconsistency in interpretation across different regions, entities and their auditors will result.
Response: The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The subjectivity involved in the Critical Cyber Asset identification requirement will be addressed in future releases of these Standards. The 15		

Organization	Yes or No	Question 4 Comment
minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve reliability impacts. The SDT believes the Responsible Entity can provide evidence demonstrating how certain systems in a generating plant will not have a reliability impact within 15 minutes.		
Northeast Utilities	Agree	
CenterPoint Energy	Agree	
LCEC	Disagree	This section of R2 makes the requirement very confusing: For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. If this is intended to be further clarification for generating units only, there should be a paragraph for this alone. In addition, the basis for "within 15 minutes" is not defined and could lead to subjectivity in the interpretation of this requirement.
Response: The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact. Please refer to the guidance document for the basis for the 15 minute limitation.		
Xcel Energy		
Great River Energy	Agree	
ITC Holdings	Disagree	New CIP-002-4 R2 Critical Cyber Asset Identification- The revisions made are introducing confusion while only identifying the inclusion of Cyber assets with delimited (arbitrarily) time for impact: "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Either a new qualification and characteristic of Critical Cyber Assets is created or the

Organization	Yes or No	Question 4 Comment
		existing characteristics shall be updated to explicitly address the type of Cyber Asset.
Response: The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
Public Utility District No. 1 of Clark County	Agree	
TransAlta		
Exelon	Agree	
AECI	Agree	
N.W. Electric Power Cooperative, Inc.	Agree	
Central Electric Power Cooperative	Agree	
Central Electric Power Cooperative	Agree	
M & A Electric Power Cooperative	Agree	
LCRA Transmission Services Corporation	Agree	
Sho-Me Power Electric Cooperative	Agree	

Organization	Yes or No	Question 4 Comment
KAMO Power	Agree	
United Illumiinating	Agree	
Constellation Energy Commodities Group	Agree	
Associated Electric Cooperative, Inc.	Agree	
KAMO Electric Cooperative	Agree	
Northeast Missouri Electric Power Cooperative	Agree	
NW Electric Power Cooperative, Inc.	Agree	
Sierra Pacific Power d/b/a NV Energy	Agree	
Sho-Me Power Electric Cooperative	Agree	
SDG&E	Disagree	Neither the mapping document nor the draft language contain the phrase "...performing a function...". That phrase has been added to this document and should be removed. The standard should focus on those cyber assets that are essential to the operation of the Critical Assets.
Response: Thank you for your comment. The phrase "…performing a function…" does not exist in the posted Standard.		
Central Lincoln	Disagree	Central Lincoln believes that "annually" should be further clarified. It could be interpreted to either be once in a calendar year or once every twelve months. If the later is intended, suggest specifying a maximum interval to allow for review dates that could otherwise fall on weekends, holidays, or during emergencies. We suggest a maximum interval of 15 months. It remains unclear how cyber assets that are newly discovered to be critical

Organization	Yes or No	Question 4 Comment
		during these reviews are to be treated, as discussed below.
Response: The phraseology you are concerned about is in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.		
Northeast Missouri Electric Power Cooperative	Agree	
National Rural Electric Cooperative Association (NRECA)		
Tampa Electric	Agree	We agree with the proposed language, however if this version does not pass and changes need to be made, we would strongly recommend bright line criteria for Critical Cyber Assets and a CCA identification methodology. In the absence of such criteria and associated methodology we expect inconsistency across entities, and would recommend the language here be modified as follows: "the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units via common mode failure that in aggregate exceeds Attachment 1, criterion 1.1 within 15 minutes."
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.		
M&A Electric Power Cooperative	Agree	
MEAG Power	Agree	
Associated Electric Cooperative, Inc.	Agree	
Associated Electric Cooperative, Inc.	Agree	

Organization	Yes or No	Question 4 Comment
FirstEnergy Corp	Agree	
Minnesota Power	Agree	
Manitoba Hydro	Disagree	The term “this list” could be interpreted as referring only to the generation units in the previous sentence. Suggest changing to “the list of associated Critical Cyber Assets essential to the operation of the Critical Asset(s)”. The 15-minute “real-time” criterion should be applied to all Critical Cyber Assets, not just generation cyber assets.
Response: Thank you for your comments. Requirement R2 has been changed to clarify the issues presented. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
American Transmission Company	Agree	
Ameren	Disagree	The word “associated” could mean anything to do with a Critical Assets which is too broad of a term and needs to be defined to avoid confusion. The phrase "could adversely impact the reliable operation" is unclear and vague. What magnitude of "adverse impact" should be considered? Also what is being defined as the Reliable Operation? This phrase should be more clearly defined, otherwise it could introduce different interpretations in the compliance audits.
Response: Thank you for your comments. The term “associated” is used in the same manner in the currently enforceable CIP-002-3. The phrase “adversely impact” limits the scope of the evaluation of Critical Cyber Assets to those that can affect the reliable operation of 1500MW or more of generation at a single plant location.		
BGE	Agree	Clarify wording by moving generation comments to the end of paragraphs, as follows: “Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. Each Responsible Entity shall review this list at least annually, and update it as necessary .For each group of generating units identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any

Organization	Yes or No	Question 4 Comment
		combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:....."
Response: Thank you for your comment. Requirement R2 has been changed to clarify the issues presented.		
Beaches Energy Services (of City of Jacksonville Beach, FL)	Disagree	BES believes that a similar "shared Cyber Assets" criterion needs to be applied at a substation for transmission Facilities emanating from that substation in a similar fashion as is described for power plants. For instance, if the entire substation is found to be a Critical Asset as a result of application of Attachment 1, a single microprocessor-based relay isolated and only operating one non-critical transmission Facility should not be swept into the standards. Instead, only shared Cyber Assets controlling the entire critical substation should be a Critical Cyber Asset. FMPA recommends avoiding the use of the term "Annual" due to the ambiguity of the term. Instead something like "Once a calendar year, but no longer than 15 months" may be more appropriate.
Response: Thank you for your comments. The term Transmission Facilities can be applied to either the entire substation or each Facility or group of Facilities connected to that substation, as determined by the entity. This would allow an entity which has multiple voltage levels at a single substation to either declare the entire substation as a Critical Asset or only the portion of the substation that qualifies under any particular criterion. The shared cyber asset qualifier only applies to criterion 1.1 because it refers to a group of generating units. The phraseology you are concerned about (annual) is in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version		
We Energies	Agree	Although we agree with the proposed Requirement R2, We are concerned that the document "CIP-002-4 Cyber Security - Critical Cyber Asset Identification: Rationale and Implementation Reference Document" actually appears to provide more rationale and guidance on Critical Assets than Critical Cyber Assets.
Response: Thank you for your comments. The guidance document title was chosen based on the title of CIP-002-4.		
City Utilities of Springfield, MO	Agree	SPRM agrees with the proposed Requirement.
Response:		

Organization	Yes or No	Question 4 Comment
Thank you for your comments.		
National Grid	Agree	Same as for Q3. If the intent is for entities to retain documentation of the basis for categorization, this should be explicitly stated in the standard. Otherwise the only documentation retained may be the list of assets.
Response: Thank you for your comment. Please see our response to Question 3. Please refer to the posted reference document for guidance on documentation.		
Lincoln Electric System	Agree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
Response: Thank you for your comments.		
Southwest Power Pool Regional Entity	Disagree	The requirement states "the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." The requirement should be modified to state" the only Cyber Assets that must be considered are those shared Cyber Assets that if destroyed, degraded, misused or otherwise rendered unavailable, could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1." The fifteen minute criterion is not necessary and could result in disagreement between the entity and the auditor over whether the impact could occur within the fifteen minute versus a longer period. Removing the fifteen minute window and clarifying that the entity must consider both loss and misuse removes that ambiguity. As with R1, the first instance of Critical Cyber Asset determination under CIP-002-4 needs to take place on or before the effective date of the standard. This affords the entity a minimum of six months to complete the required assessment. (The auditors will seek evidence based on this expectation, so placing it in the standard or accompanying guidance will remove any ambiguity such as that experienced with Version 1 of the standards) The current qualifying criterion R2.1 states "The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter." Although well intentioned, this does not adequately address risk exposure. While a given Critical Cyber Asset might not communicate itself with Cyber Assets outside of the Electronic Security Perimeter, the network it is connected to may well have connectivity to external networks. That external connectivity offers a vector for compromise through an intermediary system that both the external network and the Critical Cyber Asset are connected to. This exclusion should only apply in the

Organization	Yes or No	Question 4 Comment
		instance where the network employing a routable protocol is completely isolated from any network not enclosed within the same Electronic Security Perimeter. Additionally, please accept and consider the following comments for Requirement R3. The comment form does not provide an opportunity for "other" considerations. R3: The requirement states "The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets." This statement should be modified to read "The senior manager or delegate(s) shall approve upon creation or modification, but at least annually if no changes were required, the list of Critical Assets and the list of Critical Cyber Assets." R3: The requirement includes the statement "...approval of the risk-based assessment methodology..." As a risk-based assessment methodology is no longer required, this reference needs to be removed.
Response: Thank you for your comments. The SDT believes the Responsible Entity can more easily demonstrate whether or not a system can impact the reliable operation within 15 minutes as opposed to "if destroyed, degraded, misused or otherwise rendered unavailable, could adversely impact the reliable operation." The approach taken by the SDT does not preclude the evaluation of CCA for "if destroyed, degraded, misused or otherwise rendered unavailable, could adversely impact the reliable operation." The implementation plan (posted on the Project 2008-06 project page at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html) specifies the proposed compliance schedule of the standards and requirements. Regarding modifications to the routable protocol exception, the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. Modifications to the Critical Cyber Asset list may be made as necessary but the list still only requires annual approval. The SDT believes the annual approval period provides the appropriate level of governance in the process. References to the risk-based assessment will be removed prior to the next ballot.		
Indianapolis Power & Light	Agree	
Constellation Power Generation	Agree	
Independent Electricity System Operator	Disagree	The "15 minutes" timeline outlined in the second sentence of R2 is not clear to us as the content was interpreted differently by different individuals within our environment; hence, we ask the drafting team to consider clarifying the wordings around this.

Organization	Yes or No	Question 4 Comment
Response: Thank you for your comments. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact. Requirement R2 has been changed to add clarity around the issue. Please refer to the guidance document posted on the Project 2008-06 project page at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html for additional information.		
American Electric Power (AEP)	Disagree	The language used is a little difficult to follow. "...could adversely impact the reliable operation" suggest adding "if lost or disrupted through cyber attacks." In addition, R2.2 uses the term control center (also used in attachment 1) that is not a NERC defined term. This will introduce ambiguity to implementation. There has been ongoing confusion regarding the difference between "control centers" and "control rooms." We do not believe that a "control room" at a power plant or a substation would be considered a "control center." There is language in the NERC Security Guideline for Electricity Sector: Identifying Critical Assets document that the SDT should consider and incorporate into the NERC Glossary. We suggest that parts of Requirement 3 could be added to requirements 1 and 2 and then Requirement 3 could be removed.
Response: Thank you for your comments. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. Please refer to the guidance document posted on the Project 2008-06 project page at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html for clarification between "control center" and "control room." At this time, the SDT is choosing not to add terms to the NERC Glossary. We feel defining terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.		
Orlando Utilities Commission	Disagree	There are many functions critical to reliable operations that are not essential to the operation of a particular critical asset. Situational awareness is one such example. It would appear that these assets would not be identified under the version of this requirement.
Response: Thank you for your comment. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology.		
Oglethorpe Power Corporation	Disagree	The wording requiring that adverse effect occur within 15 minutes is a good start, but at the moment, it appears to only pertain to generation related cyber assets. The requirement should be reworded to extend this to all cyber assets, as it makes sense that if 15 minutes is the criterion for generation, it should be the

Organization	Yes or No	Question 4 Comment
		criterion for other cyber assets, or if it is not, some other, explicit criterion should be included.
Response: Thank you for your comment. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		
Brazos Electric Power Cooperative, Inc.	Disagree	The sentences dealing with the generating unit cyber asset should be moved to a sub-requirement.
Response: Thank you for your comment. The SDT considered this and other proposals and changed the wording of R2 based on industry input.		
Midwest ISO	Agree	
Duke Energy	Agree	
Seminole Electric Cooperative, Inc.	Disagree	See prior comments on Attachment 1
Response: Thank you for your comment. See response to question 2.		
Progress Energy	Agree	
Orlando Utilities Commission	Agree	There are many functions critical to reliable operations that are not essential to the operation of a particular critical asset. Situational awareness is one such example. It would appear that these assets would not be identified under the version of this requirement.
Response: Thank you for your comment. The SDT agrees. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology.		
New York Independent System Operator		

Organization	Yes or No	Question 4 Comment
Cowlitz County PUD	Agree	
Orlando Utilities Commission	Disagree	Question 4 Comments:Â Â Â Â There are many functions critical to reliable operations that are not essential to the operation of a particular critical asset. Situational awareness is one such example. It would appear that these assets would not be identified under the version of this requirement.
Response: Thank you for your comment. The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology.		
Kansas City Power & Light	Disagree	The phrase “within 15 minutes” introduces audit uncertainty and is subject to debate and disagreement between Registered Entities and Audit Teams. Recommend an improved delineation that is intended that is measurable and auditable.
Response: Thank you for your comment. The SDT believes the Responsible Entity can demonstrate whether or not a system can impact the reliable operation within 15 minutes. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.		

5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement.

Summary Consideration: In response to question 5, some commenters asked for new terms to be added to the NERC Glossary. At this time, the SDT is choosing not to add terms to the NERC Glossary since defining these terms would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect. APPA's review of the associated implementation plan for CIP-002-4 identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. Several entities requested that the implementation plans be combined. A NERC Standard Implementation Plan address assets that are in place and applicable the date the standard becomes effective. It is retired once the Implementation Plan is completed. The Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses assets that are identified in the future and future Registered Entities and is an ongoing plan that has no expected retirement date. Some entities asked for a provision for extensions to the implementation plan for good cause. The suggested modification proposes an exception process to a mandatory standard, and the SDT refers the entities to the discussion on technical feasibility exceptions in the FERC Order. Specifically, the oversight framework which must be in place is summarized in paragraph 222. Some commenters felt the implementation plan was too aggressive. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC Approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset. Some entities requested a 24 month implementation after effective date of standard, and indicated that the proposed plan was too complicated. The SDT has simplified the implementation plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.

Organization	Yes or No	Question 5 Comment
Northeast Power Coordinating Council	No	Need a Control Center definition to clarify 1) control center, 2) control system, 3) backup control center, 4) backup control. Since the current, approved Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses most of the criteria covered by CIP-002-4, request that relevant content be moved to that document. Creating a separate Implementation Plan is redundant and will cause confusion for entities trying to address appropriate timelines.

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comments. At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. A NERC Standard Implementation Plan address assets that are in place and applicable the date the standard becomes effective. It is retired once the Implementation Plan is completed. The Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses assets that are identified in the future and future Registered Entities and is an ongoing plan that has no expected retirement date.		
City of Garland	Yes	
NRG Energy Inc.	Yes	
APPA CIP-002-4 Task Force	No	Proposed Implementation Plan APPA Comments: APPA's review of the associated Implementation Plan for CIP-002-4 has identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. We would request modification to the Implementation Plan such that it reflects the intent of the Reliability Standard. The Implementation Plan does not adequately address when a "New Asset" that does meet the CIP-002-4 criteria for being a Critical Asset after its commissioning will need to be in compliance. APPA believes that the intent of the Reliability Standard indicates that the post-commissioned New Asset will become a Newly Identified Critical Asset upon the subsequent Annual Review and only at the time of this Annual Review. Further that the timeline associated with this Newly Identified Critical Asset starts with the date of the Annual Review. We raise this point because we are concerned about the potential impact for confusion associated with multiple review dates or continuous reviews of the assets contained within numerous CIP activities. If an entity has multiple Cyber Assets, the entity would likely have multiple Annual Reviews dates.
Response: Thank you for your comments. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. The text reference was removed from the Implementation Plan.		

Organization	Yes or No	Question 5 Comment
IRC Standards Review Committee	No	Since the current, approved Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses most of the criteria covered by CIP-002-4, request that relevant content be moved to that document. Creating a separate Implementation Plan is redundant and will cause confusion for entities trying to address appropriate timelines.
Response: Thank you for your comments. A NERC Standard Implementation Plan address assets that are in place and applicable the date the standard becomes effective. It is retired once the Implementation Plan is completed. The Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses assets that are identified in the future and future Registered Entities and is an ongoing plan that has no expected retirement date.		
Bonneville Power Administration	No	If this version requires more substations to be identified as Critical Assets, then we believe that the proposed implementation is too aggressive. Physical Security Perimeters are expensive and it may not be possible to fund these modifications in the short timeframe for compliance. A 3-year implementation period would be more appropriate.
Response: Thank you for your comment. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC Approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
PSEG Companies	No	PSEG believes that overall, the proposed implementation plan for the Version 4 standards is appropriate and makes sense. PSEG does suggest the following addition: Reasonably unforeseen circumstances may occur that prevent strict compliance within the timeframes envisioned in the implementation plan. By allowing for Regional Entity review of the need for an extension of time, registered entities can be afforded necessary flexibility without unduly slowing the implementation. In the implementation plan insert before "Prior Version Standard Retirements" the following new section: Extension for Good Cause Critical Cyber Assets shall be compliant by the schedule set forth herein unless a Regional Entity grants prior approval of an extension for specified Critical Cyber Assets for good cause based on scheduling constraints or other constraints beyond the control of the Registered Entity.

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Pepco Holdings, Inc - Affiliates	No	We suggest the following addition: In the implementation plan insert before "Prior Version Standard Retirements" the following new section: Extension for Good Cause Critical Cyber Assets shall be compliant by the schedule set forth herein unless a Regional Entity grants prior approval of an extension for specified Critical Cyber Assets for good cause based on scheduling constraints or other constraints beyond the control of the Registered Entity.
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
MRO's NERC Standards Review Subcommittee	No	The implementation plan is overly complex and confusing. It is not clear when the “Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4” applies versus when the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” applies. Does the former document apply only upon the approval of the CIP-002-4 and, then, subsequently, the latter implementation plan apply? The flow chart appears to show this. If this is the intention, we suggest that should be made clear somewhere in the document. As the document is written now, it is not clear.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Santee Cooper	No	Eighteen months from the effective date of version 4 may not be a reasonable amount of time for certain entities. For example, if an entity recently produced a vulnerability/risk assessment under the current standard, the entity should be allowed up to 12 months before the criteria in Attachment 1 is applied. The

Organization	Yes or No	Question 5 Comment
		SDT should consider compliance being effective no earlier than 18 months after completion of the entity's most recent vulnerability/risk assessment (or application of Attachment 1 after the standard is approved for implementation).
Response: Thank you for your comment. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Dominion	Yes	Dominion has the following comments: While we recognize that there will be a tremendous amount of effort and coordination required to protect large generation units and transmission facilities to implement the requirements, we agree with the current implementation plan. However we would be concerned of any shortening of the implementation schedule because the logistics required for design and procurement engineering, outage scheduling, and lead times for the acquisition of material, equipment and labor.
Response: Thank you for your comment.		
Edison Mission Marketing and Trading	Yes	
Florida Municipal Power Agency	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
PNGC Power	No	Again we associate ourselves with NRECA's request for a 24 month implementation after effective date of standard. Plus the ability to extend the deadline if conditions warrant.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		

Organization	Yes or No	Question 5 Comment
The SDT believes an additional provision to allow for extenuating circumstances carries the same oversight requirements as the TFE process.		
WECC		
Southern Company	No	However, the Implementation Plan (under the section titled "Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4"), requires that Critical Cyber Assets "which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4." This requirement does not provide sufficient time for the Responsible Entity to achieve compliance. For example, under this provision, an asset that is identified on the last day of the 18 month period would only have 1 day to achieve compliance, which is not a sufficient amount of time for implementation. To allow Responsible Entities sufficient time to reach compliance, the SDT should consider deleting the section titled "Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4." The result of this change would mean that all Critical Cyber Assets that are newly identified after the Effective Date of CIP-002-4 would be subject to compliance as set forth in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. Southern believes this streamlined approach will be easier to implement than having a separate timeline for Critical Cyber Assets that are newly identified within the first 18 months after the Effective Date of CIP-002-4.This suggestion is contingent upon the SDT's adoption of Southern's comments to Question 6 which establishes a uniform 24 month implementation schedule or a different implementation deadline granted by the Regional Entity for good cause, rather than different timelines for different requirements. Furthermore, it is impossible for large utilities to enumerate and verify all the CCAs within 6 months, due to the number of CAs requiring analysis of common systems.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval. The SDT believes an additional provision to allow for extenuating circumstances carries the same oversight requirements as the TFE process.		
Encari, LLC	Yes	
Arizona Public Service	No	Revising the set of Standards CIP-002 through CIP-009 to Version 4, as described in these drafts, seems to conflict with the (almost) concurrent SAR process to revise CIP-005-4. The ultimate outcome and impact to the proposed implementation plan is unclear. AZPS is unable to determine at this time which CIP-005-4 version is likely to be in effect for this proposed Version 4 implementation plan. It seems highly desirable to incorporate the intended changes to CIP-005-4, as indicated by the SAR revision, into the larger set of

Organization	Yes or No	Question 5 Comment
		Version 4 updates. The revision timelines and resulting implementation and auditability implications are of great concern. AZPS urges the 706 SDT team to consider reasonable adjustment in the implementation of the posted Standards CIP-002 through CIP-009 to Version 4 to ensure incorporation and synchronization of the Project 2010-15 â€• Urgent Action Revisions to CIP-005-3 (http://www.nerc.com/filez/standards/SAR-Urgent_Action_Revisions%20to%20CIP-005-3.html) â€• CIP-005 version changes in order to minimize confusion and potential implementation conflict to the industry.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
Edison Electric Institute	No	EEI believes that overall, the proposed implementation plan for the Version 4 standards is appropriate and makes sense. We suggest the following addition: In the implementation plan insert before "Prior Version Standard Retirements" the following new section: Extension for Good Cause Critical Cyber Assets shall be compliant by the schedule set forth herein unless a Regional Entity grants prior approval of an extension for specified Critical Cyber Assets for good cause based on scheduling constraints or other constraints beyond the control of the Registered Entity.
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Tennessee Valley Authority (TVA)		
PacifiCorp	Yes	
OGE	Yes	
FMPA	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
South Carolina Electric and Gas	Yes	
Pinellas County Resource Recovery Facility	Yes	
Central Lincoln	Yes	
Edison Mission Marketing and Trading	Yes	
SPS Consulting Group Inc.	No	I do not see an Implementation Plan on the Project site other than the one for Nuclear facilities that has already been approved by FERC.
Response: Thank you for your comment. The Implementation plan can be found on the 2008-06 project page under the version 4 documents. The Version 4 page is located at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html		
Tacoma Power	No	Tacoma Power would like to identify the following as errors in the proposed implementation plan: Under Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4 U.S. Nuclear Power Plant Facilities and also All Other Critical Cyber Assets, the implementation plan reads, “the latter of.” Tacoma Power believes the SDT meant to say “the later of.” Tacoma Power also suggests that the Category 2 timelines for compliance with CIP-005-4 through CIP-009-4 be extended to 24 months as these standards could require capital improvements necessary to comply with the standards.
Response:		

Organization	Yes or No	Question 5 Comment
Thank you for your comments. The text you reference has been removed. Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Green Country Energy	Yes	
Illinois Municipal Electric Agency	No	IMEA supports comments submitted by the American Public Power Association.
Response: Thank you for your comments. Please see the SDT response to APPA comments.		
Minnkota Power Cooperative	No	CIP-005-4 is going through a bit of a different process, but its implementation plan is the same as the rest of the Version 4 standards. Based on the number of configuration changes that may be required for communications outside of the ESP for currently designated CCAs, we request a longer implementation plan for CIP-005-4 in terms of currently identified CCAs.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
Horizon Wind Energy	Yes	
Union Power Partners LP	Yes	
MidAmerican Energy Company	Yes	
North Carolina Membership Corporation	No	NCEMC agrees with NRECA comment “The proposed implementation plan is incredibly confusing and must be greatly simplified. NRECA recommends an implementation plan that requires compliance within 24 months of the effective date of the standard, with a provision that allows entities to request extensions of this deadline for extenuating circumstances. Additional confusion could come from the fact that CIP-002-4 and its implementation plan could be filed with FERC by the end of 2010 and then CIP-010 and CIP-011 and its implementation plan could be submitted to FERC some time in 2011. With two sets of changes to these standards and related implementation plans being filed with FERC within months, the required implementation of these standards could be very confusing and challangeing to navigate."

Organization	Yes or No	Question 5 Comment
Response: Thank you for your comments. Please see our response to NRECA comments.		
Hydro One Networks Inc.	Yes	
Dynegy Inc.	No	This is way to hard to follow and understand. The Implementation Plan is 18 pages. Suggest doing it on one page. I can't tell with certainty when I am due to be compliant. This must be clear so entities don't miss their initial compliance due date because they misunderstood when they were supposed to be compliant.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Matrikon Inc.		
Northeast Utilities	Yes	
CenterPoint Energy	Yes	
LCEC	Yes	
Xcel Energy	No	The proposed 18 months implementation is not realistic in all cases. Additional flexibility is needed to account for complex changes that can not be completed in that short of a timeframe.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Great River Energy	No	For newly identified Critical Assets of a given type (Control Center, Generation Plant, Substation) the entity will be given a longer period of time than if it is not the first instance for that entity.
Response:		

Organization	Yes or No	Question 5 Comment
Thank you for your comments. Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
ITC Holdings	Yes	
Public Utility District No. 1 of Clark County	Yes	
TransAlta		
Exelon	No	In the "Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4", although page 2 explicitly addresses CCA compliance for Nuclear generators as being 18 months after the CIP-002-4 effective date (with certain exceptions for refueling outages) the flow-chart logic on page 3 does not achieve the same result. That is, if a nuclear generator is not a CA for CIP-002-3 and thus has no CCAs, the second decision diamond would result in a "no" and exit to "Newly Identified CCAs and Newly Registered Entities" and not the 18-month compliance milestone. Suggest the second diamond be reworded to include the logic of no current CA's, or explicitly refer to nuclear GO/GOP.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
AECI	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		

Organization	Yes or No	Question 5 Comment
N.W. Electric Power Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Central Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Central Electric Power Cooperative	No	Comments: In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
M & A Electric Power	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not

Organization	Yes or No	Question 5 Comment
Cooperative		going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
LCRA Transmission Services Corporation	Yes	
Sho-Me Power Electric Cooperative	No	Comments: In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
KAMO Power	No	Comments: In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		

Organization	Yes or No	Question 5 Comment
United Illumiinating	No	the proposed implementation plan for the Version 4 standards is appropriate and makes sense. We suggest the following addition: In the implementation plan insert before "Prior Version Standard Retirements" the following new section: Extension for Good Cause Critical Cyber Assets shall be compliant by the schedule set forth herein unless a Regional Entity grants prior approval of an extension for specified Critical Cyber Assets for good cause based on scheduling constraints or other constaints beyond the control of the Registered Entity.
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Constellation Energy Commodities Group	No	I would suggest that it should not be assumed that an entity with an existing CIP program would require a shorter implementation period than an entity without existing Critical Cyber Asset. The period should be the same at 24 months.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		

Organization	Yes or No	Question 5 Comment
KAMO Electric Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Northeast Missouri Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
NW Electric Power Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Sierra Pacific Power d/b/a NV	Yes	

Organization	Yes or No	Question 5 Comment
Energy		
Sho-Me Power Electric Cooperative	No	Comments: In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
SDG&E	No	What schedule will CIP005 follow given the proposed revisions to that standard?
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
Central Lincoln	Yes	
Northeast Missouri Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
National Rural Electric Cooperative Association	No	The proposed implementation plan is incredibly confusing and must be greatly simplified. NRECA recommends an implementation plan that requires compliance within 24 months of the effective date of the standard, with a provision that allows entities to request extensions of this deadline for extenuating

Organization	Yes or No	Question 5 Comment
(NRECA)		circumstances. Additional confusion could come from the fact that CIP-002-4 and its implementation plan could be filed with FERC by the end of 2010 and then CIP-010 and CIP-011 and its implementation plan could be submitted to FERC some time in 2011. With two sets of changes to these standards and related implementation plans being filed with FERC within months, the required implementation of these standards could be very confusing and challangeing to navigate.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval. The SDT believes an additional provision to allow for extenuating circumstances carries the same oversight requirements as the TFE process.		
Tampa Electric	Yes	
M&A Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
MEAG Power	Yes	
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of		

Organization	Yes or No	Question 5 Comment
2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
FirstEnergy Corp	No	FirstEnergy believes that overall the Implementation Plan consisting of 15 pages is overly complex and could be greatly simplified. We recognize that for the most part the SDT attempted to make minimal conforming changes to an already approved Implementation Plan. However, much of the Implementation Plan discusses scenarios and examples of company mergers and a recognition that separate Critical Asset identification processes may exist between the companies and time is needed to assess a going-forward position on Critical Asset determinations. The discussion is applicable when companies developed and maintained their own unique Risk Based Assessment Methodologies, however, under the "bright-line" Critical Asset determinations performed with CIP-002-4 it should be expected that minimal differences will result, otherwise we have not achieved the industry consistency desired under this "bright-line" criteria. If the criteria in Attachment 1 are crisp and clear the only potential item open to asset owner subjectivity are the assets classified as Critical Assets under criterion 1.16 which reads "Any additional assets that the Responsible Entity deems appropriate to include." It is FE's view that the resulting merged Responsible Entity could adjust 1.16 based on what it "deems necessary" and any CIP-003 through CIP-009 compliance required of the resulting "newly identified Critical Cyber Assets" simply follow Category 1 or Category 2 as appropriate. To simplify the Implementation Plan we encourage the SDT to reconsider the need for material presented under the section titled "Newly Registered Entity Scenarios" on pages 8 through 11 and the continued need for Table 3. There are earlier references to "Newly Registered Entities and Table 3 that exist on page 2 that could potentially be removed as well.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8		

Organization	Yes or No	Question 5 Comment
calendar quarters after regulatory approval. The section on Newly Registered Entities scenarios has been revised to address your concerns.		
Minnesota Power	No	Minnesota Power believes that overall, the proposed implementation plan for the Version 4 standards is appropriate and makes sense. We suggest the following addition: In the implementation plan insert before "Prior Version Standard Retirements" the following new section:" Extension for Good Cause Critical Cyber Assets shall be compliant by the schedule set forth herein unless a Regional Entity grants prior approval of an extension for specified Critical Cyber Assets for good cause based on scheduling constraints or other constraints beyond the control of the Registered Entity."
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized . We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Manitoba Hydro	No	The proposed 18 month timeframe is too short for the industry to meet compliance for a group of new CCAs. Although the existing approved Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities provides up to 18 months to reach compliance for some requirements under an existing program, the identification of new CCAs would distributed over time, both throughout the entity and throughout the industry. This new CIP-002-4 compliance date could cause a sudden increase in the number of new CCAs throughout the industry, which may not have the resources to meet this sudden compliance burden. Some consideration should be given to the types of environments and their unique challenges when establishing compliance dates. The flowchart on page 3 needs to be revised, since the CAs are identified by the Criteria in Attachment #1, not the CCAs. Suggest changing to "Are the CCAs associated with CAs newly identified by the Criteria...".
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
American Transmission	No	ATC agrees the implementation schedule in general, should allow for sufficient time (18 months from effective date; 24 months from FERC approval date) for Category 2 entities to become compliant with CIP-003 through

Organization	Yes or No	Question 5 Comment
Company		CIP-009. However, we suggest an extension should be allowed for good cause if approved by the Regional Entity.
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Ameren	No	Under All Facilities Other Than U.S. Nuclear Power Plants Facilities Page 2, Line 3, the words "within the first 18 months following the Effective Date of CIP-002-4" should be removed. The way that this paragraph is currently written if an Entity identifies a Critical Cyber Assets in the 17 month following the Effective Date of CIP-002-4, the Entity would have to be compliant with all of CIP Version 4 the next month (18 months after the Effective Date of CIP-002-4). In the CCA-Based Decision Tree the third diamond (Is the identification of the CCA within 18 months of the Effective Date of CIP-002-4) should be removed. Also, the implementation schedule should be changed to give an Entity at least 6 months following the Effective Date of CIP-002, R1 to comply with CIP-002, R2 and R3. This would allow an Entity time to inventory all its CCAs, especially for generation assets, this would give the Entity about a year to develop their inventory of CCAs.
Response: Thank you for your comments. The Implementation Plan has been modified to reference the Effective Date which is 8 calendar quarters after regulatory approval for CIP-002-4 through CIP-009-4.		
BGE	Yes	Strong need for clarifying wording: - Time line given should be clearly labeled that it is ONLY if the FERC approves the standard in the first quarter 2011. - Remove the words EXAMPLE and SAMPLE to describe the Scenarios, in the table and in the text. Perhaps a statement that this list of scenarios is not "ALL INCLUSIVE" would be correct in this situation. - With the time allowed in tables used for varying scenarios, it seems that a similar amount of time should be used for new Cyber Assets never before in service rather than requiring "Compliant upon Commissioning". There is a focused effort and many changes required to bring a Cyber Asset into compliance and there may be an impact on operability and reliability if delays occur in implementation.

Organization	Yes or No	Question 5 Comment
		- Is Scenario used in the text and the table to mean different things? - P. 11 uses a term bulk power system - is this to mean Bulk Electric System? - There is no table for Scenario 3. - Provide an explanation that Auditably Compliant is a term no longer used as all entities who must be compliant should expect that during any audit after approval of the standard, information will be reviewed for compliance
Response: Thank you for your comments. - The guidance document was modified to address the concerns about time line and list of scenarios not being all-inclusive. - The technical security requirements should be considered as part of the acquisition and commissioning process for a Critical Cyber Asset. - The implementation plan references scenarios for both newly registered entities and newly identified Critical Cyber Assets. The scenarios referenced in Table 1 of this document refer to Critical Cyber Assets. - The reference has been changed to Bulk Electric System - References to Auditably Compliant have been removed.		
Beaches Energy Services (of City of Jacksonville Beach, FL)	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
We Energies	Yes	
City Utilities of Springfield, MO	No	SPRM agrees with the comments from the APPA Task Force.
Response: Thank you for your comment. Please see the SDT response to APPA comments.		
National Grid	Yes	

Organization	Yes or No	Question 5 Comment
Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
Response: Thank you for your comment. Please see the SDT response to MRO NERC Standards Review Subcommittee		
Southwest Power Pool Regional Entity	Yes	
Indianapolis Power & Light	Yes	
Constellation Power Generation	No	Constellation Power Generation believes that 18 months to implement these requirements is not enough time. Based on the number of self reports and compliance issues regarding the CIP standards, it is evident that not enough time was given to entities in the implementation phase. Therefore, Constellation Power Generation suggests that the SDT extend the implementation time to 24 months.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Independent Electricity System Operator	Yes	
American Electric Power (AEP)	Yes	
Orlando Utilities Commission	Yes	
Oglethorpe Power Corporation	Yes	
Brazos Electric Power Cooperative, Inc.		
Midwest ISO	No	The implementation plan is overly complex and confusing. It is not clear when the “Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4” applies versus when the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” applies.

Organization	Yes or No	Question 5 Comment
		Does the former document apply only upon the approval of the CIP-002-4 and, then, subsequently, the latter implementation plan apply? The flow chart appears to show this. If this is the intention, we suggest that should be made clear somewhere in the document. As the document is written now, it is not clear. Some of the paths in the flowchart in figure 1 of the draft guidance rationale and implementation reference document appear to be missing. We are placing our comment regarding R3 here because there are no other appropriate questions that ask about R3 or anything else that has not been covered in the other questions. R3 requires conforming changes. In the last sentence, it still refers to the Responsible Entity keeping a signed and dated record of the senior manager's approval of the risk-based methodology.
Response: Thank you for your comments. Your understanding of the implementation plan is correct. We will make changes to the guidance document to make this more evident. We will correct figure 1 on the guidance document. The issue you raise with R3 has been corrected.		
Duke Energy	Yes	
Seminole Electric Cooperative, Inc.	No	The proposed implementation plan is incredibly confusing and must be greatly simplified. SEC recommends an implementation plan that requires compliance within 24 months of the effective date of the standard, with a provision that allows entities to request extensions of this deadline for extenuating circumstances. Additional confusion could come from the fact that CIP-002-4 and its implementation plan could be filed with FERC by the end of 2010 and then CIP-010 and CIP-011 and its implementation plan could be submitted to FERC some time in 2011. With two sets of changes to these standards and related implementation plans being filed with FERC within months, the required implementation of these standards could be very confusing and challenging to navigate.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Progress Energy	No	NERC needs to address what happens if an entity's annual assessment falls within 30-60 days of the approval date. That situation would require the entity to execute their version 3 Risk Based Assessment

Organization	Yes or No	Question 5 Comment
		Methodology, and then immediately (or concurrently) do an assessment using the version 4 criteria. A solution to the above problem is to make version 4 effective on the first day of the calendar quarter after regulatory approval, and then require compliance with CIP-002-4 and for CCAs previously identified 6 months after the effective date, and compliance for CIP-003-4 through CIP-009-4 for newly identified CCAs 24 months after the effective date.
Response: Thank you for your comments. The SDT does not believe that it is overly burdensome to have entities adjust the timing of their review to accommodate the transition to CIP version 4.		
Orlando Utilities Commission	Yes	
New York Independent System Operator		
Cowlitz County PUD	No	There will be some confusion between the Annual Assessment and Commissioning of new assets. The timeline for compliance should begin after the Annual Assessment is concluded finding the new added asset as critical.
Response: Thank you for your comments. Entities are expected to be compliant with CIP-002-4 to CIP 009-4 upon commissioning of a new Critical Cyber Asset.		
Orlando Utilities Commission	Yes	
Kansas City Power & Light	No	It should be 24 months to establish compliance with this proposed standard for any newly identified critical assets and newly identified cyber critical assets by the application of this proposed standard. Circumstances can change that are not predetermined but result in an asset qualifying as a critical asset.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		

6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement.

Summary Consideration: In response to question 6, some commenters noted conforming changes that needed to be made in the implementation plan for newly identified CCAs and Responsible Entities. The SDT made these changes and will post them in the next ballot. Most other comments were similar to those offered in question 5, for which the SDT offered the same responses.

Organization	Yes or No	Question 6 Comment
Northeast Power Coordinating Council	No	Agree as long as an Entity can request additional time due to a large increase in identified assets - something like a TFE with a mitigating plan. Throughout the Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities, Critical Asset identification is noted as a "Critical Asset identification process". Process should be stricken as it is not supported by the wording of the requirement R1. Request that the term "Bulk Electric System" be used in the document in place of "bulk power system". This is in keeping with the standard and the NERC glossary. The inclusion of CIP-005-4 R6 in the proposed changes is dependent upon concurrent industry, BOT, and FERC approval of CIP-005-4 and CIP-002-4. If these approvals do not occur at the same time, request removal of CIP-005-4 R6 from Table 2. Request clarification regarding the implementation plan for prior versions of the CIP standards. Will implementation plans of approved CIP standards remain in place until those standards are retired and audit periods have closed for those versions?

Response:

Thank you for your comments. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.

The requirements of CIP-002-4 R1 still require a process of Critical Asset Identification.

Agreed. The SDT has changed the reference from bulk power system to Bulk Electric System.

Organization	Yes or No	Question 6 Comment
Regarding CIP-005-4, NERC will make conforming changes dependent on the results of the CIP-005-4 Urgent Action SAR ballot. Upon the Effective Date for version 4 Standards, previous implementation plans are no longer in effect.		
City of Garland	Yes	
NRG Energy Inc.	Yes	
APPA CIP-002-4 Task Force	No	Proposed Implementation Plan APPA Comments: APPA's review of the associated Implementation Plan for CIP-002-4 has identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. We would request modification to the Implementation Plan such that it reflects the intent of the Reliability Standard. The Implementation Plan does not adequately address when a "New Asset" that does meet the CIP-002-4 criteria for being a Critical Asset after its commissioning will need to be in compliance. APPA believes that the intent of the Reliability Standard indicates that the post-commissioned New Asset will become a Newly Identified Critical Asset upon the subsequent Annual Review and only at the time of this Annual Review. Further that the timeline associated with this Newly Identified Critical Asset starts with the date of the Annual Review. We raise this point because we are concerned about the potential impact for confusion associated with multiple review dates or continuous reviews of the assets contained within numerous CIP activities. If an entity has multiple Cyber Assets, the entity would likely have multiple Annual Reviews dates.
Response: Thank you for your comments. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. The text reference was removed from the Implementation Plan.		
IRC Standards Review Committee	No	See comments to Question 1 above and the proposed Attachment 1.
Response: Thank you for your comments. Please refer to response to Question 1.		

Organization	Yes or No	Question 6 Comment
Bonneville Power Administration	Yes	Yes, these look appropriate.
PSEG Companies	No	Although the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities reflect historical precedent in terms of FERC approval, PSEG believes that with the exception of nuclear facilities, it would be better to simply have a uniform 18 month implementation deadline for newly identified CCAs and Responsible Entities, rather than different timelines for different requirements. Nuclear timelines are subject to NRC requirements and the necessity of accomplishing some tasks only during refueling outages and thus are appropriately kept on a separate schedule. Other comment: As posted, the revised CIP-002-4 has the following language (Page 2):R3. Annual Approval -The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R23 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) Recommendation: References to risk-based assessment methodology should be removed.
Response: Thank you for your comments. Due to the limited scope of version 4, the SDT is only making conforming changes to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. The references to risk-based assessment have been removed.		
Pepco Holdings, Inc - Affiliates	No	Although the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities reflect historical precedent in terms of FERC approval, we believe that with the exception of nuclear facilities discussed under U.S. Nuclear Power Plant Facilities, it would be better to simply have a uniform18 month implementation deadline for newly identified CCAs and Responsible Entities, rather than different timelines for different requirements.
Response: Thank you for your comments. Due to the limited scope of version 4, the SDT is only making conforming changes to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.		

Organization	Yes or No	Question 6 Comment
MRO's NERC Standards Review Subcommittee	No	For newly identified Critical Assets, a 24 month implementation is provided for Entities that have never identified a Critical Asset under the version 3 standards, with only 18 months provided for Entities with existing Critical Assets. We believe the SDT has developed a sound approach with this delineation. However, we also believe the 24 month implementation should be expanded to include Entities that may have existing Critical Assets, but have never identified a Critical Asset of a given type, i.e., generating unit, transmission facility, control center, etc. For example, if a company had a control center that was previously identified as critical, but version 4 results in their first generating unit being identified, then we would propose that they be given 24 months to become compliant as they are working on their first generating unit. Also, many sections of the new identified CCAs and responsible entities still reflect the former risk-based assessment methodology. For example, in the Implementation Milestone Categories on page 4, there is a discussion regarding a change in power flows causing non-critical assets to become Critical Assets. Under the new criteria, there is no evaluation of power flows. A better example would be referencing criterion 1.3 in CIP-002-4 Attachment 1 - "When a PC or TP newly identifies a generation Facility that is required for reliability purposes." In the section discussing mergers, there is discussion of how to combine Critical Asset identification processes. Again, this was written assuming entities needed to combine their risk-based assessment methodologies and resolve any differences. There is no need for discussion of combining these processes with bright line criteria. Furthermore, there are other statements in the merger section that need to be updated to reflect the bright line criteria as well. The paragraph from the merger section in 3 (a) that begins with "Registered Entities are encouraged when combining separate risk-based Critical Asset identification processes..." should be removed since there should be no reduction in Critical Assets from a merger with bright line criteria. For Table 3, how do we know which column applies? Is it based on category 1 and category 2 as shown in Table 2 and described in the Implementation Milestone Categories and Schedules? If so, then column headings should be added to Table 3 to clarify.

Response:

Thank you for your comments. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.

The SDT agrees the text you reference still reflects the risk-based assessment methodology and have made those conforming changes.

Table 3 only applies to entities registered after the CIP-002-4 Effective Date. The column headings reflect 12 months and 24 months respectively after the date of registration.

Organization	Yes or No	Question 6 Comment
Santee Cooper	No	The implementation plans are confusing and long. The industry would probably prefer one document, with tables or charts that depict all possible scenarios, combining all elements of all implementation plans.
Response: Thank you for your comment. In the general case, a Responsible Entity has at least 6 months to comply with CIP-002-4 and 18 additional months to comply with CIP-003-4 through CIP-009-4. The SDT believes the additional specification is appropriate to provide Responsible Entities reasonable time to comply in the respective scenarios. A NERC Standard Implementation Plan address assets that are in place and applicable the date the standard becomes effective. It is retired once the Implementation Plan is completed. The Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses assets that are identified in the future and future Registered Entities and is an ongoing plan that has no expected retirement date.		
Dominion	No	Certain Table 2 Milestone Category 2 time frames do not appear to give due consideration to the effort that may be involved with implementation. For example, providing training is allowed 18 months where as establishing physical and electronic security, which is likely to involve engineering and construction, is only allowed 12 months. Dominion suggests time frames for Category 2 physical and electronic security be changed to 18 months.
Response: Thank you for your comment. The 18 month time frame for training recognizes all other cyber security controls must be in place prior to training personnel.		
Edison Mission Marketing and Trading	Yes	
Florida Municipal Power Agency	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
PNGC Power	No	Same as #5

Organization	Yes or No	Question 6 Comment
WECC		
Southern Company	No	Southern believes the SDT should implement a uniform 24 month implementation deadline, or a different implementation deadline granted by the Regional Entity for good cause, rather than different timelines for different requirements.
Response: Thank you for your comment. The suggested modification proposes an exception process to a mandatory standard. We refer to the discussion on technical feasibility exceptions in the FERC Order, specifically, to the oversight framework which must be in place that is summarized in paragraph 222. The SDT believes the effective date provides a reasonable timeframe for entities to become compliant with CIP-002-4 through CIP-009-4, which would preclude the need to implement a burdensome exception process for the industry.		
Encari, LLC	Yes	
Arizona Public Service	Yes	
Edison Electric Institute	No	Although the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities reflect historical precedent in terms of FERC approval, we believe that with the exception of nuclear facilities, it would be better to simply have a uniform18 month implementation deadline for newly identified CCAs and Responsible Entities, rather than different timelines for different requirements. We have additional input: The Following Functional entities to be added to the applicability section: Planning Coordinator, Transmission Planner. Issue: As posted, the revised CIP-002-4 has the following language (Page 2):R3. Annual Approval -The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 , R2, and R23 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) Recommendation: References to risk-based assessment methodology should be removed.

Organization	Yes or No	Question 6 Comment
Response: Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. There are no requirements in version 4 of the CIP Cyber Security Standards for Planning Coordinators and Transmission Planners. References to the risk-based assessment methodology have been removed.		
Tennessee Valley Authority (TVA)		
PacifiCorp	Yes	: While PacifiCorp agrees with the proposed revisions to this implementation plan, the Company does suggest an alternative approach that may remove the complications that are created with the current multiple implementation schedules. It would be simpler if all responsible entities had 18 months from the effective date of CIP-002-4 to bring any newly identified Critical Cyber Assets (CCAs) into compliance with CIP-003-4 through CIP-009-4, regardless of the reason for which new CCAs are identified.
Response: Thank you for your comment. As written in the Implementation Plan, all entities have 18 months from the effective date of CIP-002-4 to bring new CCAs into compliance. Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
OGE	Yes	
FMPA	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
South Carolina Electric and Gas	Yes	
Pinellas County Resource	Yes	

Organization	Yes or No	Question 6 Comment
Recovery Facility		
Central Lincoln	Yes	
Edison Mission Marketing and Trading	Yes	
SPS Consulting Group Inc.	No	See answer to Question 5.
Response: Thank you for your comment.		
Tacoma Power	Yes	Tacoma Power agrees with the proposed revisions to the implementation plan.
Response: Thank you for your comment.		
Green Country Energy	Yes	
Illinois Municipal Electric Agency	No	IMEA supports comments submitted by the American Public Power Association.
Response: Thank you for your comment.		
Minnkota Power Cooperative	Yes	As mentioned in question 5, our concern is over the implementation of current CCAs.
Response: Thank you for your comment.		
Horizon Wind Energy	Yes	
Union Power Partners LP	Yes	

Organization	Yes or No	Question 6 Comment
MidAmerican Energy Company	Yes	MidAmerican Energy Company agrees with the proposed revisions to the implementation plan but would like to suggest an 18 month compliance deadline regardless of whether the responsible entity has previously identified CCAs. MidAmerican Energy Company believes a uniform 18 month deadline would reduce confusion among responsible entities and provide a simplified method of compliance for CIP-002-4 going forward.
Response: Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.		
North Carolina Membership Corporation	No	See answer to item 5 above
Response: Thank you for your comment.		
Hydro One Networks Inc.	Yes	
Dynegy Inc.	No	See previous comments to Question 5.
Response: Thank you for your comment.		
Matrikon Inc.		
Northeast Utilities	Yes	
CenterPoint Energy	Yes	
LCEC	Yes	

Organization	Yes or No	Question 6 Comment
Xcel Energy		
Great River Energy	No	Our rationale is the same for CCAs as it is for CAs. See comment for question 5 above.
Response: Thank you for your comment.		
ITC Holdings	Yes	
Public Utility District No. 1 of Clark County	Yes	
TransAlta		
Exelon	Yes	
AECI	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
N.W. Electric Power Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response:		

Organization	Yes or No	Question 6 Comment
Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Central Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Central Electric Power Cooperative	No	Comments: : In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
M & A Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security		

Organization	Yes or No	Question 6 Comment
Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
LCRA Transmission Services Corporation	Yes	
Sho-Me Power Electric Cooperative	No	Comments: : In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
KAMO Power	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
United Illumiinating	No	Although the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities reflect historical precedent in terms of FERC approval, we believe that with the exception of nuclear facilities discussed , it would be better to simply have a uniform18 month implementation deadline for newly identified CCAs and Responsible Entities, rather than different timelines for different requirements.
Response: Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in		

Organization	Yes or No	Question 6 Comment
implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.		
Constellation Energy Commodities Group	No	I would suggest that it should not be assumed that an entity with an existing CIP program would require a shorter implementation period than an entity without existing Critical Cyber Asset. The period should be the same at 24 months.
Response: Thank you for your comment. In the general case, a Responsible Entity has at least 6 months to comply with CIP-002-4 and 18 additional months to comply with CIP-003-4 through CIP-009-4. The SDT believes the additional specification is appropriate to provide Responsible Entities reasonable time to comply in the respective scenarios.		
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
KAMO Electric Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		

Organization	Yes or No	Question 6 Comment
Northeast Missouri Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
NW Electric Power Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Sierra Pacific Power d/b/a NV Energy	Yes	
Sho-Me Power Electric Cooperative	No	Comments: : In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security		

Organization	Yes or No	Question 6 Comment
Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
SDG&E	Yes	
Central Lincoln	No	Central Lincoln supports the APPA Comments: APPA's review of the associated Implementation Plan for CIP-002-4 has identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. We would request modification to the Implementation Plan such that it reflects the intent of the Reliability Standard. The Implementation Plan does not adequately address when a "New Asset" that does meet the CIP-002-4 criteria for being a Critical Asset after its commissioning will need to be in compliance. APPA believes that the intent of the Reliability Standard indicates that the post-commissioned New Asset will become a Newly Identified Critical Asset upon the subsequent Annual Review and only at the time of this Annual Review. Further that the timeline associated with this Newly Identified Critical Asset starts with the date of the Annual Review. Additional Central Lincoln Comments: Central Lincoln notes that the APPA comment regarding commissioning new equipment is not the only path to new CCAs, since an existing cyber asset may become critical due to other system changes. Immediate non-compliance with all CIP requirements and resulting enforcement action is not a way to encourage compliance.
Response: Thank you for your comments. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. The text reference was removed from the Implementation Plan. An existing cyber asset becoming critical due to other system changes would be a Category 2 Scenario if (i) the system change was not planned and (ii) the entity has an existing CIP Cyber Security program. If the system change were planned and implemented by the entity, then the Critical Cyber Asset implementation is part of the planning process.		
Northeast Missouri Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.

Organization	Yes or No	Question 6 Comment
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
National Rural Electric Cooperative Association (NRECA)	No	See answer to Question 5.
Response: Thank you for your comments. Please refer to response to question 5.		
Tampa Electric	Yes	
M&A Electric Power Cooperative	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
MEAG Power	No	MEAG supports the APPA's comments submitted to the NERC CIP standard drafting team.
Response: Thank you for your comments.		
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new

Organization	Yes or No	Question 6 Comment
		requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Associated Electric Cooperative, Inc.	No	In some cases there could be a significant outlay of financial and staff resources and current budgets are not going to allow start of implementation of a project until the following year. Therefore, it should be 12 months to identify Critical Assets and 36 months to complete implementing CIPs 003-009. This will provide entities enough time to request financing and the additional staffing that may be required to perform the new requirements of the CIP standards.
Response: Thank you for your comments. The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
FirstEnergy Corp	No	See our Question 5 response.
Response: Thank you for your comments.		
Minnesota Power	Yes	
Manitoba Hydro	No	Suggest changing wording in the first sentence of the fifth paragraph of page 1 "...application of the Critical Asset identification..." to " ... application of Critical Asset Criteria for the identification of Critical Assets...".
Response: Thank you for your comment. The SDT agrees to make that conforming change.		
American Transmission Company	No	Support EEI's comment. Although the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities reflect historical precedent in terms of FERC approval, we believe that, with the exception of nuclear facilities, it would be better to simply have a uniform18 month implementation

Organization	Yes or No	Question 6 Comment
		deadline for newly identified CCAs and Responsible Entities, rather than different timelines for different requirements.
Response: Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.		
Ameren	No	This schedule is too aggressive and is also very confusing. In this regard, we suggest the following: The time frame for Entities to be compliant for Category 2 should be changed to 18 months for all periods instead of 6, 12, or 18 months. This would match the 18 month proposed period for the Version 4 implementation schedule which gives every requirement other than CIP-002 18 months instead of different time periods. This will also prevent requirements that are dependent on actions in other requirements to not have different time periods to be compliant, for example CIP-005 R1.5 and CIP-006 R2.2. Another example is CIP-004-4 R1 where an Entity will not know who needs on-going reinforcement in sound security practices if the Entity has not established a list of who has authorized cyber or physical access per the CIP-004-4 R4 requirement. Should the Category 1 Milestone and Category 2 Milestone for CIP-003-4 R2 match to be either N/A or existing?
Response: Thank you for your comments. The SDT believes the timeframes for Category 2 Critical Cyber Assets are appropriate given the preexisting cyber security program. Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.		
BGE	No	See specific comments below:- Terms “Responsible Entity and Responsibility Entity” are capitalized and is not defined throughout the Implementation Plan. If these are NERC terms, please put their definition in the NERC Glossary of Terms - BGE believes that the difference in time in Milestone Category 1 and Milestone Category 2 in Table 2 should not exist as the implementation of developing an Electronic Security Perimeter and protecting new CCAs is equally as challenging for a company who already has CCAs that are protected. - Time line given should be clearly labeled that it is ONLY if the FERC approves the standard in the first

Organization	Yes or No	Question 6 Comment
		quarter 2011. - Remove the words EXAMPLE and SAMPLE to describe the Scenarios, in the table and in the text. Perhaps a statement that this list of scenarios is not "ALL INCLUSIVE" would be correct in this situation. - Does the "Compliant upon Commissioning" make sense for new Cyber Assets never before in service? - Is Scenario is used in the text and the table to mean different things. Please clarify.
Response: Thank you for your comments. The term "Responsibility Entity" has been corrected. While "Responsible Entity" is not a NERC Glossary term, it is acceptable to use the term in the Implementation Plan corresponding to the applicable standard. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes an entity that does not have existing CCAs must go through significantly more internal process changes and technical training than would an entity that already has an existing CIP Cyber Security Program. Your suggested modifications to the guideline have been incorporated. The SDT believes "Compliant upon Commissioning" makes sense for a new Cyber Asset which becomes a Critical Cyber Asset for an entity who has an existing CIP Cyber Security Program. The implementation plan references scenarios for both newly registered entities and newly identified Critical Cyber Assets. The scenarios referenced in Table 1 of this document refer to Critical Cyber Assets.		
Beaches Energy Services (of City of Jacksonville Beach, FL)	No	Without knowing the outcome of CIP-005-4, we cannot support the implementation plan.
Response: Thank you for your comments. The implementation plan associated with the Urgent Action SAR for modifications to CIP-005-3 will be drafted as part of a separate ballot and is outside the scope of this SDT. If both ballots pass, then the SDT anticipates NERC will merge the documents for filing with FERC.		
We Energies	No	We believe that it would be better to simply have a uniform 18 month implementation deadline for newly identified CCAs rather than have different timelines for different requirements. This will simplify reporting and streamline efforts to become fully compliant. We understand that nuclear timelines are subject to NRC requirements and the necessity of accomplishing some tasks only during refueling outages appropriately dictates a separate schedule for them.

Organization	Yes or No	Question 6 Comment
Response: Thank you for your comment. Because FERC has already approved this plan, and due to the limited scope, the SDT is only making conforming changes at this time. The SDT believes the shorter timeframe for entities having Critical Cyber Assets in version 3 reflects the organizational knowledge and expertise in implementing the cyber security requirements. Also, all entities have 24 months from regulatory approval to implement the requirements of the CIP Cyber Security Standards.		
City Utilities of Springfield, MO	No	SPRM agrees with the comments from the APPA Task Force.
Response: Thank you for your comments.		
National Grid	Yes	
Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
Response: Thank you for your comments.		
Southwest Power Pool Regional Entity	No	Remove all references to the term "Auditably Compliant (AC)". FERC has held that the requirements are auditable and enforceable as of the Compliant (C) milestone date. The auditors are aware of the nuances of required data retention and other time-specific requirements and will seek evidence of compliance appropriately. The idea that entities have an entire year after the Compliant milestone date to actually become compliant has caused considerable issues with previous versions of the standard.
Response: Thank you for your comments. The SDT agrees that Auditably Compliant is no longer relevant to version 4 of the CIP Cyber Security Standards and references have been removed.		
Indianapolis Power & Light	Yes	
Constellation Power Generation	No	Constellation Power Generation believes that 18 months to implement these requirements is not enough time. Based on the number of self reports and compliance issues regarding the CIP standards, it is evident that not enough time was given to entities in the implementation phase. Therefore, Constellation Power Generation

Organization	Yes or No	Question 6 Comment
		suggests that the SDT extend the implementation time to 24 months.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Independent Electricity System Operator	Yes	
American Electric Power (AEP)	Yes	AEP suggests a less complex approach if possible.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Orlando Utilities Commission	Yes	
Oglethorpe Power Corporation	Yes	
Brazos Electric Power Cooperative, Inc.		
Midwest ISO	No	Many sections of the new identified CCAs and responsible entities still reflect the former risk-based assessment methodology. For example, in the Implementation Milestone Categories on page 4, there is a discussion regarding a change in power flows causing non-critical assets to become Critical Assets. Under the new criteria, there is no evaluation of power flows. A better example would be referencing criterion 1.3 in CIP-002-4 Attachment 1 - "When a PC or TP newly identifies a generation Facility that is required for reliability purposes." In the section discussing mergers, there is discussion of how to combine Critical Asset identification processes. Again, this was written assuming entities needed to combine their risk-based assessment methodologies and resolve any differences. There is no need for discussion of combining these processes with bright line criteria. The paragraph from the merger section in 3 (a) that begins with "Registered Entities are encouraged when combining separate risk-based Critical Asset identification processes..." should be removed since there should be no reduction in Critical Assets from a merger with bright line criteria.For Table 3, how do we know which column applies? Is it based on category 1 and category 2 as shown in Table 2 and described in the

Organization	Yes or No	Question 6 Comment
		Implementation Milestone Categories and Schedules? If so, then column headings should be added to Table 3 to clarify.
Response: The SDT agrees the text you reference still reflects the risk-based assessment methodology and have made those conforming changes. Table 3 only applies to entities registered after the CIP-002-4 Effective Date. The column headings reflect 12 months and 24 months respectively after the date of registration.		
Duke Energy	No	The implementation plan for newly identified Critical Cyber Assets is confusing. It appears that Critical Cyber Assets which are newly identified during the first 18 months following the Effective Date of CIP-002-4 must be compliant 18 months following the Effective Date of CIP-002-4 (or 6 months following refueling for items requiring a refueling outage to complete). However, if an entity identified a new Critical Cyber Asset near the end of the 18 month period, there might not be enough time left to achieve compliance. To allow for this possibility, the implementation plan for Critical Cyber Assets identified following the Effective Date of CIP-002-4 should require compliance at the latter of 18 months following the Effective Date of CIP-002-4, or the applicable Category 2 milestone date.
Response: Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.		
Seminole Electric Cooperative, Inc.	No	See response to 5 above.
Response: Thank you for your comment.		
Progress Energy	Yes	
Orlando Utilities Commission		
New York Independent System Operator		

Organization	Yes or No	Question 6 Comment
Cowlitz County PUD	Yes	
Orlando Utilities Commission	Yes	
Kansas City Power & Light	No	The Implementation Plan does not adequately address when a "New Asset" that does meet the CIP-002-4 criteria for being a Critical Asset after its commissioning will need to be in compliance. APPA believes that the intent of the Reliability Standard indicates that the post-commissioned New Asset will become a Newly Identified Critical Asset upon the subsequent Annual Review and only at the time of this Annual Review. Further that the timeline associated with this Newly Identified Critical Asset starts with the date of the Annual Review.

Response:

Thank you for your comments. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. The text reference was removed from the Implementation Plan.

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Window Open
October 20-November 3, 2010

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Instructions
Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Two errors were discovered in the versions of the standards posted for comment and review on September 20, 2010 and these errors have been corrected in the clean and redline versions of the standard posted for ballot on October 20, 2010. To see the two errors, review the yellow highlighted text in the redline versions of the standards posted on October 20, 2010.

- In CIP-002-4 Requirement R3, the phrase, "approval of the risk-based methodology," was removed.
- In the applicability section of CIP-008-4, the "nuclear exclusion" was removed.

Project 2008-06 — Cyber Security 706
A set of proposed changes to CIP-002-3 - Cyber Security — Critical Cyber Asset Identification, associated implementation plans, and conforming changes to several other CIP standards have been posted for stakeholder ballot. These are considered, "Version 4 CIP Standards." The drafting team also developed and posted a mapping document to show the translation of requirements from CIP-002-3 to CIP-002-4, and a guidance document to assist in applying the proposed CIP-002-4 standard.

The proposed CIP-002-4 provides a significant improvement to CIP-002-3 by including a specific list of criteria for entities to use in identifying their critical assets.

The previously approved versions of CIP-002 relied on entities to develop their own critical asset identification methodology, and have led to unequal assessments of critical assets between entities in a region, and between regions. This subjectivity has led some external observers to question how assessments were produced, and has contributed to distrust of the entire critical asset identification process. The revised standard provides uniformity to the critical asset identification process for all entities as well as uniformity and predictability to the audit process. As envisioned, each entity will apply the criteria against its assets to determine exactly which side of the "bright line" they fall. The bright-line thresholds are justified based on overall impact to Bulk Electric System reliability, adding further clarity to the critical asset identification process. The bright-line criteria were developed based on stakeholder comments on CIP-010, which is currently under development.

Recognizing that protecting the cyber assets critical to the electric utility's infrastructure is also critical to national and international security, the revisions to CIP-002 are being advanced ahead of other improvements to the remaining set of CIP standards. The remaining CIP standards all rely on a complete and accurate identification of those assets that are critical to reliability. Because entities are so tightly interconnected, a vulnerability that seems

insignificant to a single entity can place the entire grid in a state of vulnerability.

Each of the CIP standards (CIP-003-3 through CIP-009-3) contains at least one reference to CIP-002-3. To maintain clarity, CIP-003-3 through CIP-009-3, have had conforming changes made so that all cross references within the set of standards are to "CIP Version 4" standards. *(CIP-005-4 - Cyber Security — Electronic Security Perimeter is posted separately, with a set of proposed revisions for Urgent Action under Project 2010-15. If CIP-005-4 is not approved as an Urgent Action, it will be returned to this set of CIP standards.)*

Transition from Reliability Standards Development Procedure Version 7 to Standard Processes Manual

Under the Reliability Standards Development Procedure Version 7, consensus was built with successive formal comment periods, followed by a 30-day pre-ballot review, followed by an initial ballot, and then a recirculation ballot. The intent was to use stakeholder views submitted through the formal comment periods to achieve consensus, and then to confirm that consensus during the balloting. This process did not allow a drafting team to make any changes to a standard between ballots, which incented teams to avoid making improvements once a standard had gone through an initial ballot. If a team made a change between ballots, then the standard was required to be posted for a new comment period and then another pre-ballot review and another initial ballot. Finally, if there were no more changes made to the standard, a recirculation ballot was conducted to confirm consensus.

Under the new Standard Processes Manual, consensus is achieved through parallel comment and ballot periods. Successive comment and ballot periods are conducted until there is consensus – and then a recirculation ballot is conducted to confirm that consensus. There is no 30-day pre-ballot review period, and drafting teams are encouraged to make revisions to the standard between successive ballots to improve the quality of the standard.

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

Further details are available on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity

NERC
Regional Entity

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_in
Ballot Period:	10/20/2010 - 11/3/2010
Ballot Type:	Initial
Total # Votes:	384
Total Ballot Pool:	410
Quorum:	**93.66 % The Quorum has been reached**
Weighted Segment Vote:	43.33 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	113	1	48	0.462	56	0.538	5	4
2 - Segment 2.	11	0.7	2	0.2	5	0.5	3	1
3 - Segment 3.	93	1	29	0.341	56	0.659	4	4
4 - Segment 4.	30	1	6	0.25	18	0.75	3	3
5 - Segment 5.	87	1	30	0.4	45	0.6	5	7
6 - Segment 6.	51	1	20	0.426	27	0.574	1	3
7 - Segment 7.	1	0.1	1	0.1	0	0	0	0
8 - Segment 8.	10	0.8	3	0.3	5	0.5	0	2
9 - Segment 9.	5	0.3	3	0.3	0	0	0	2
10 - Segment 10.	9	0.9	6	0.6	3	0.3	0	0
Totals	**410**	**7.8**	**148**	**3.379**	**215**	**4.421**	**21**	**26**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Negative	View
1	American Electric Power	Paul B. Johnson	Negative	View
1	American Transmission Company, LLC	Jason Shaver	Affirmative	View
1	Arizona Public Service Co.	Robert D Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Negative	View
1	Avista Corp.	Scott Kinney	Affirmative	
1	Baltimore Gas & Electric Company	John J. Moraski	Affirmative	View

1	BC Transmission Corporation	Gordon Rawlings	Negative	View
1	Beaches Energy Services	Joseph S. Stonecipher	Negative	View
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	View
1	Central Electric Power Cooperative	Michael B Bax	Negative	View
1	Central Maine Power Company	Brian Conroy		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	View
1	City of Vero Beach	Randall McCamish	Negative	
1	City Utilities of Springfield, Missouri	Jeff Knottek	Negative	
1	Clark Public Utilities	Jack Stamper	Negative	View
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	
1	Commonwealth Edison Co.	Gregory Campbell	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	View
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	John K Loftis	Negative	View
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S.	Larry Monday		
1	East Kentucky Power Coop.	George S. Carruba	Negative	View
1	Edison Electric Institute	David Batz	Abstain	View
1	Empire District Electric Co.	Ralph Frederick Meyer	Negative	View
1	Entergy Corporation	George R. Bartlett	Negative	View
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	View
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	View
1	GDS Associates, Inc.	Claudiu Cadar	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	View
1	Hoosier Energy Rural Electric Cooperative, Inc.	Robert Solomon		
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	View
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Negative	View
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	View
1	Keys Energy Services	Stan T. Rzad	Negative	View
1	Lake Worth Utilities	Walt Gill	Negative	
1	Lakeland Electric	Larry E Watt	Negative	View
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam	Negative	
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	View
1	M & A Electric Power Cooperative	William Price	Negative	View
1	Manitoba Hydro	Michelle Rheault	Negative	View
1	MEAG Power	Danny Dees	Negative	View
1	Metropolitan Water District of Southern California	Ernest Hahn	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi Woodward	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Affirmative	
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Negative	View
1	National Grid	Saurabh Saksena	Affirmative	View
1	Nebraska Public Power District	Richard L. Koch	Negative	View
1	Nevada Power Co.	James McMorran		
1	New York Power Authority	Arnold J. Schuff	Negative	
1	North Carolina Electric Membership Corp.	Gary Ofner	Abstain	View
1	Northeast Missouri Electric Power Cooperative	Kevin White	Negative	View
1	Northeast Utilities	David H. Boguslawski	Affirmative	View
1	Northern Indiana Public Service Co.	Kevin M Largura	Negative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	View

1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Negative	
1	Omaha Public Power District	Douglas G Peterchuck	Affirmative	
1	Oncor Electric Delivery	Michael T. Quinn	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Negative	View
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Abstain	
1	PacifiCorp	Colt Norrish	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	Frank F. Afranji	Affirmative	
1	Potomac Electric Power Co.	Richard J Kafka	Negative	View
1	PowerSouth Energy Cooperative	Larry D. Avery	Negative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Progress Energy Carolinas	Sammy Roberts	Negative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	View
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Negative	View
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch	Negative	View
1	Rochester Gas and Electric Corp.	John C Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Negative	View
1	Salt River Project	Robert Kondziolka	Negative	View
1	Santee Cooper	Terry L. Blackwell	Negative	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Negative	View
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	South Texas Electric Cooperative	Richard McLeon	Abstain	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Negative	View
1	Southern Illinois Power Coop.	William G. Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	
1	Southwestern Power Administration	Gary W Cox	Negative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Negative	View
1	Transmission Agency of Northern California	James W. Beck	Negative	View
1	Tri-State G & T Association, Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Negative	View
1	Westar Energy	Allen Klassen	Affirmative	View
1	Western Area Power Administration	Brandy A Dunn	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Negative	View
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Negative	View
2	California ISO	Gregory Van Pelt	Abstain	View
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Negative	View
2	Independent Electricity System Operator	Kim Warren	Negative	View
2	ISO New England, Inc.	Kathleen Goodman		
2	Midwest ISO, Inc.	Jason L Marshall	Negative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Negative	
3	Alabama Power Company	Richard J. Mandes	Negative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Negative	
3	American Electric Power	Raj Rana	Negative	View
3	American Public Power Association	Nathan Mitchell	Negative	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen	Negative	
3	APS	Steven Norris	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Negative	View
3	Atlantic City Electric Company	James V. Petrella	Negative	
3	Avista Corp.	Robert Lafferty		
3	BC Hydro and Power Authority	Pat G. Harrington	Negative	View
3	Blue Ridge Power Agency	Duane S. Dahlquist	Abstain	
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte	Negative	View

3	Central Lincoln PUD	Steve Alexanderson	Negative	View
3	City of Bartow, Florida	Matt Culverhouse	Negative	
3	City of Clewiston	Lynne Mila	Negative	
3	City of Farmington	Linda R. Jacobson	Negative	View
3	City of Green Cove Springs	Gregg R Griffin	Negative	View
3	City of Leesburg	Phil Janik	Negative	
3	City Water, Light & Power of Springfield	Roger Powers	Negative	View
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	View
3	Consumers Energy	David A. Lapinski	Abstain	
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Edwin Les Barrow		
3	Delmarva Power & Light Co.	Michael R. Mayer	Negative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F Gildea	Negative	View
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	East Kentucky Power Coop.	Sally Witt	Negative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Solutions	Kevin Querry	Affirmative	View
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Negative	
3	Florida Power Corporation	Lee Schuster	Negative	
3	Gainesville Regional Utilities	Kenneth Simmons	Negative	
3	Georgia Power Company	Anthony L Wilson	Negative	View
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	View
3	Great River Energy	Sam Kokkinen	Negative	
3	Gulf Power Company	Gwen S Frazier	Negative	View
3	Hydro One Networks, Inc.	David L Kiguel	Negative	View
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Negative	View
3	Kansas City Board of Public Utilities	Robert D Adam	Affirmative	
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Negative	View
3	Lakeland Electric	Mace Hunter	Abstain	
3	Lincoln Electric System	Bruce Merrill		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Abstain	
3	M & A Electric Power Cooperative	Stephen D Pogue	Negative	View
3	Madison Gas and Electric Co.	Darl Shimko	Negative	View
3	Manitoba Hydro	Greg C. Parent	Negative	View
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Negative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Negative	View
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Negative	View
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone	Affirmative	
3	North Carolina Municipal Power Agency #1	Denise Roeder	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Negative	View
3	Northern Indiana Public Service Co.	William SeDoris	Negative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	View
3	NW Electric Power Cooperative, Inc.	David McDowell	Negative	View
3	Ocala Electric Utility	David T. Anderson	Negative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	View
3	Orlando Utilities Commission	Ballard Keith Mutters	Negative	View
3	Owensboro Municipal Utilities	Richard H. Chapman	Negative	View
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	Vincent J. Catania	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	View
3	Potomac Electric Power Co.	Robert Reuter		
3	Progress Energy Carolinas	Sam Waters	Negative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Negative	View
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Negative	View
3	Salt River Project	John T. Underhill	Negative	View
3	San Diego Gas & Electric	Scott Peterson	Negative	View

3	Santee Cooper	Zack Dusenbury	Negative	
3	Seattle City Light	Dana Wheelock	Affirmative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Negative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Negative	View
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	View
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Affirmative	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Negative	View
3	Xcel Energy, Inc.	Michael Ibold	Negative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Abstain	
4	American Municipal Power - Ohio	Kevin Koloini	Negative	
4	American Public Power Association	Allen Mosher	Negative	View
4	Central Lincoln PUD	Shamus J Gamache	Negative	View
4	City of Clewiston	Kevin McCarthy	Negative	
4	City of New Smyrna Beach Utilities Commission	Timothy Beyrle	Negative	
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring		
4	Florida Municipal Power Agency	Frank Gaffney	Negative	View
4	Fort Pierce Utilities Authority	Thomas W. Richards	Negative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	View
4	Illinois Municipal Electric Agency	Bob C. Thomas	Negative	View
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	
4	Integrys Energy Group, Inc.	Christopher Plante	Negative	View
4	LaGen	Richard Comeaux	Negative	View
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Negative	View
4	National Rural Electric Cooperative Association	Barry Lawson	Abstain	View
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	View
4	Oklahoma Municipal Power Authority	Terri Pyle	Abstain	
4	Old Dominion Electric Coop.	Mark Ringhausen	Negative	View
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Negative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Negative	View
4	Seattle City Light	Hao Li	Affirmative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Negative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	View
4	Wisconsin Energy Corp.	Anthony Jankowski	Negative	View
4	Wisconsin Public Power Inc.	Patrick Connors	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Negative	View
5	Allegheny Energy Supply Company, LLC	Robert Loy	Affirmative	
5	Amerenue	Sam Dwyer	Negative	
5	APS	Mel Jensen	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson	Negative	View
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma	Negative	View
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Chelan County Public Utility District #1	John Yale	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Grand Island	Jeff Mead	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	View
5	City of Tallahassee	Alan Gale	Negative	View
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	View
5	Consumers Energy	James B Lewis	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert B Stevens	Negative	View
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Negative	View

5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	East Kentucky Power Coop.	Stephen Ricker	Negative	View
5	Energy Northwest - Columbia Generating Station	Doug Ramey	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Negative	View
5	ExxonMobil Research and Engineering	Martin Kaufman	Abstain	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Florida Municipal Power Agency	David Schumann	Negative	View
5	Great River Energy	Cynthia E Sulzer	Negative	
5	Green Country Energy	Greg Froehling	Affirmative	
5	Horizon Wind Energy	Brent Hebert	Negative	View
5	Indeck Energy Services, Inc.	Rex A Roehl	Abstain	
5	Kansas City Power & Light Co.	Scott Heidtbrink		
5	Kissimmee Utility Authority	Mike Blough	Negative	
5	Lakeland Electric	Thomas J Trickey	Negative	
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Louisville Gas and Electric Co.	Charlie Martin	Abstain	
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Negative	View
5	Madison Gas and Electric Co.	Steven Schultz	Negative	View
5	Manitoba Hydro	S N Fernando		
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Negative	View
5	Michigan Public Power Agency	James R. Nickel		
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Nebraska Public Power District	Don Schmit	Negative	View
5	New York Power Authority	Gerald Mannarino	Negative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Negative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle DAntuono	Affirmative	View
5	Oglethorpe Power Corporation	Scott McGough	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Negative	View
5	Orlando Utilities Commission	Richard Kinas	Negative	View
5	Pacific Gas and Electric Company	Richard J. Padilla	Negative	View
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Negative	View
5	PPL Generation LLC	Annette M Bannon	Affirmative	View
5	Progress Energy Carolinas	Wayne Lewis	Negative	
5	PSEG Power LLC	Jerzy A Slusarz	Negative	View
5	Public Utility District No. 1 of Lewis County	Steven Grega	Negative	
5	Reedy Creek Energy Services	Bernie Budnik		
5	RRI Energy	Thomas J. Bradish	Negative	View
5	Sacramento Municipal Utility District	Bethany Wright	Negative	View
5	Salt River Project	Glen Reeves	Negative	View
5	Santee Cooper	Lewis P Pierce	Negative	
5	Seattle City Light	Michael J. Haynes	Affirmative	View
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Negative	
5	South Carolina Electric & Gas Co.	Richard Jones	Affirmative	
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	View
5	Tennessee Valley Authority	George T. Ballew	Negative	View
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	View
5	Tri-State G & T Association, Inc.	Barry Ingold	Negative	
5	U.S. Army Corps of Engineers Northwestern Division	Karl Bryan	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer P.E.	Affirmative	View
5	US Power Generating Company	Bohdan M Dackow		
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Negative	View
5	Wisconsin Public Service Corp.	Leonard Rentmeester	Negative	View
5	Xcel Energy, Inc.	Liam Noailles	Negative	View

6	AEP Marketing	Edward P. Cox	Negative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Negative	View
6	Arizona Public Service Co.	Justin Thompson	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Negative	View
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	View
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S Slade	Negative	View
6	Duke Energy Carolina	Walter Yeager	Affirmative	
6	Entegra Power Services	Larry W. Rodriguez	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Negative	View
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	View
6	Florida Municipal Power Agency	Richard L. Montgomery	Negative	View
6	Florida Municipal Power Pool	Thomas E Washburn	Negative	View
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	View
6	Great River Energy	Donna Stephenson	Negative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Louisville Gas and Electric Co.	Daryn Barker	Abstain	
6	Luminant Energy	Brad Jones	Negative	View
6	Madison Gas and Electric Co.	Jeffrey M Keebler	Negative	View
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	Missouri River Energy Services	Gerald A. Tielke	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Negative	View
6	NRG Energy, Inc.	Alan R. Johnson	Negative	View
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Negative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Affirmative	
6	Progress Energy	John T Sturgeon	Negative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Negative	View
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson	Negative	View
6	Salt River Project	Mike Hummel	Negative	View
6	Santee Cooper	Suzanne Ritter	Negative	
6	Seattle City Light	Dennis Sismaet	Affirmative	View
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Negative	
6	SunGard Data Systems	Christopher K Heisler		
6	Tacoma Public Utilities	Michael C Hill	Affirmative	View
6	Tampa Electric Co.	Joann Wehle	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	View
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Wisconsin Public Service Corp.	Paul Spicer		
6	Xcel Energy, Inc.	David F. Lemmons	Negative	View
7	Oak Ridge National Laboratory	Stacy Prowell	Affirmative	
8		John Kutzer		
8		Scott Hudson		
8		James A Maenner	Negative	View
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Negative	
8	Network & Security Technologies	Nicholas Lauriat	Negative	View
8	SPS Consulting Group Inc.	Jim R Stanton	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	View
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William Mitchell Chamberlain		
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	North Carolina Utilities Commission	Kimberly J. Jones		

9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Negative	View
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool Regional Entity	Stacy Dochoda	Affirmative	
10	Texas Reliability Entity	Larry D Grimm	Negative	View
10	Western Electricity Coordinating Council	Louise McCarren	Negative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Initial Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2008-06 — Cyber Security 706

The initial ballot for the following Critical Infrastructure Protection (CIP) Version 4 Standards ended on November 3, 2010:

- CIP-002-4 - Cyber Security — Critical Cyber Asset Identification
- CIP-003-4 - Cyber Security — Security Management Controls
- CIP-004-4 - Cyber Security — Personnel & Training
- CIP-006-4 - Cyber Security — Physical Security of Critical Cyber Assets
- CIP-007-4 - Cyber Security — Systems Security Management
- CIP-008-4 - Cyber Security — Incident Reporting and Response Planning
- CIP-009-4 - Cyber Security — Recovery Plans for Critical Cyber Assets

Ballot Results for Standards
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 93.66 %
Approval: 43.33 %

Since there were negative ballots that included a comment, these results are not final. A successive ballot must be conducted.

Next Steps
The drafting team will post its consideration of all comments (those submitted with a comment form, and those submitted with a ballot) and conforming changes to the standard.

Project Background
FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

Further details are available on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Consideration of Comments on Initial Ballot — Cyber Security 706 (Project 2008-06)
Date of Initial Ballot: October 20 – November 3, 2010

Summary Consideration: The majority of commenters either referred to their comments filed during the comment period or repeated those comments in the ballot. The summary responses for each question in the comment period are provided below:

Question 1: When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace?

Many of those that voted "No" contended their current risk-based methodology provided a more accurate list of Critical Assets and therefore the proposed criteria in Attachment 1 would not lead to an improvement in reliability. Often, those who commented this way also felt the criteria did not have rigorous system studies as a reliability basis.

The SDT appreciates these comments but believes that although some companies may have a very rigorous risk-based assessment, the implementation of Attachment 1 criteria will overall increase the consistency of Critical Asset identification. The Attachment 1 criteria were developed in response to an external oversight directive in the FERC Order 706. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. The "bright-line" criteria approach removes the variability of entity-defined methodologies that would prompt the need for external review.

Regarding the need for additional engineering studies, the SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. The industry provided significant feedback for the need to simplify the Critical Asset identification approach. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The results of the recent NERC data request were used to assist the team in developing the criteria in Attachment 1.

A few commenters expressed concern that changes to these standards do not address other significant issues. The SDT agrees that other changes ultimately need to be made to the body of CIP cyber security standards, and expects to resume working on those in early 2011. The scope of the changes to the interim CIP-002-4 was deliberately to minimize the impact on the industry while addressing the identified consistency issues with the Critical Asset identification method.

Question 2: CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

In response to question 2, most commenters had suggestions for improvement to the criteria for critical assets listed in Attachment 1. The SDT appreciates these comments and incorporated many of them to improve clarity and consistency. Some of the comments reflected a misunderstanding of a specific criterion, and in those instances the SDT provided additional guidance in the response to comments and modified the associated guidance document for identifying Critical Assets. The SDT believes that the implementation of Attachment 1 criteria will increase the overall consistency of Critical Asset identification. Specific summary analysis of each criterion follows, along with a summary of responses.

Criterion 1.1 defines as Critical Assets "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW." Commenters requested clarification on the phrase "single plant location." Clarity on this issue was provided in the posted guidance document. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Other commenters questioned why we no longer used Contingency Reserve in the criteria, and how the SDT arrived at the value of 1500 MW. In prior postings of CIP-002-4 and CIP-010-1 there was wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The SDT performed an informal survey of the regions and identified what the megawatt value of the reserve sharing would be for various groups. The SDT used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions.

Some commenters suggested the use of capacity factor in the criterion. The SDT debated whether to include it in this criterion. The reason the SDT ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was a concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year. After considering all of the comments, the SDT chose not change the wording of criterion 1.1.

Criterion 1.2 defines as Critical Assets "Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater." Some commenters questioned how the value of 1000 MVARs was derived. The value of 1000 MVARs used in this criterion was deemed reasonable for the purpose of determining criticality. Some commenters suggested combining criterion 1.2 with criterion 1.9. FACTS devices in 1.9 are specifically related to IROLs, whereas the reactive resources in 1.2 are not limited to IROL applications. Some commenters suggested that the limit should be set by each Regional Reliability Organization. The issue with using different MVAR values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. After considering all of the comments, the SDT chose not change the wording of criterion 1.2.

Criterion 1.3 defines as Critical Assets "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." Many commenters felt that this criterion places the responsibility for identifying the asset with the wrong entity (not the asset owner). Other commenters noted that the use of the NERC Glossary term "Adverse Reliability Impacts" would help clarify which units should be in this category. Others expressed concern that the criterion should mandate the coordination and approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. Still others stated that this criterion is open for auditors to interpret. The SDT responded that the burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability. Based on the comments received, this criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Criterion 1.4 defines as Critical Assets "Each Blackstart Resource identified in the Transmission Operator's restoration plan." Many commenters expressed concern that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. Others stated that blackstart units deemed critical should be only those identified by the TOP as specified to meet the minimum critical blackstart requirement. Some expressed concern that criterion 1.4 inadvertently provides incentive to utilities to remove resources from the restoration plan, reducing the plan's overall effectiveness.

The SDT specifically chose the NERC Glossary term “Blackstart Resources” to address the concerns expressed. A Blackstart Resource is defined as “A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator’s restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator’s restoration plan.” EOP-005-2 R1.4 states that the restoration plan must include “Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.” The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. After considering all of the comments, the SDT chose not change the wording of criterion 1.4.

Criterion 1.5 defines as Critical Assets “The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.” Some commenters stated that additional qualifying criteria should be added such as "Cranking Paths to critical units as identified in a region’s restoration plan." The SDT noted in its response that there is no longer any NERC requirement to have a region restoration plan. Others asked for clarity around where the point of multiple paths lies in the electrical system. The SDT noted in its response that the point where multiple paths exist in the Cranking Path is the step in the Transmission Operator’s restoration plan per EOP-005-2 R1.5 “Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started” where the Transmission Operator can choose between the next Facilities on the BES to energize. Some commenters expressed concern over the phrase “initial switching requirements.” Based on the comments received, this criterion has been reworded to “The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.”

Criterion 1.6 defines as Critical Assets “Transmission Facilities operated at 500 kV or higher.” Commenters expressed that voltage alone is not a sufficient criterion to determine whether or not an asset is critical to the bulk electric system. They suggested that the SDT should consider using capacity or flows based on power flow studies instead of nominal voltage level as the bright-line. The SDT responded that all Transmission Facilities operated at 500 kV or higher do not require any further qualification for their role as components of the backbone on the Interconnected BES. Furthermore, the SDT does not feel that capacity or power flow analysis (impact-based or risk-based) would lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. The SDT will take this suggestion under consideration for future revisions. After considering all of the comments, the SDT chose not change the wording of criterion 1.6.

Criterion 1.7 defines as Critical Assets “Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.” Some commenters provided the suggestion that criterion 1.7 should be reworded to "stations or substations" instead of just "stations" so that it is not implied that it only applies to power plants (stations). Others commented that the SDT should adopt a power flow-based bright-line rather than whether the station is connected to three or more other stations, similar to comments for criterion 1.6. Again, the SDT does not feel that power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. Still others commented that the statement regarding "three or more other transmission stations" is confusing. Does the criterion include stations upstream, downstream, networked or radial? Does the criterion include a radial 345 kV substation connected to a generator? The SDT response is that the intent of criterion 1.7 is to classify as Critical Assets all Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this criterion, since the criterion specifically states “three or more other transmission stations.” The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a

Critical Asset since by definition it cannot be connected to three or more transmission substations. Based on the comments received, this criterion has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations."

Criterion 1.8 defines as Critical Assets "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Some commenters stated that this criterion should be modified because loss of facilities does not cause an IROL violation. An IROL includes a limit and a time constant T_v. In order for an IROL violation to occur, the limit must be exceeded for at least the time constant T_v. Others commented that additional language should be added to clarify that the TO, LSE, etc. is not responsible for demonstrating IROLs. The SDT responded that according to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. Based on the comments received, this criterion has been reworded to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Criterion 1.9 defines as Critical Assets "Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Some commenters felt that the term FACTS should be added to the NERC Glossary. FACTS is defined by IEEE as: "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Commonly accepted terms and definitions do not require an insertion in the NERC Glossary. Some questioned why FACTS devices were singled out in the criteria. FACTS devices were singled out to ensure that there was no confusion as to whether or not they were considered Critical Assets. Other comments followed a similar vein as criterion 1.8. Based on the comments received, this criterion has been reworded to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Criterion 1.10 defines as Critical Assets "Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3." Some commenters asked for clarity about the term "directly connected." Additional questions concerned whether the language means total loss of substation or only partial. The intent of this criterion is to ensure the availability of Facilities necessary to support generation Critical Assets. Any Transmission Facility that, if lost, would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3, would need to be classified as a Critical Asset. This might include the partial or total loss of a substation. Based on the comments received, this criterion has been reworded to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3."

Criterion 1.11 defines as Critical Assets "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements." Some commenters stated that criterion 1.11 should be eliminated on the basis that is not based upon BES reliability considerations and that criticality of facilities should not be fuel specific. Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC reliability standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. Some felt that this criterion should be limited to Transmission Facilities providing offsite power requirements. Since NUC-001-2 is not limited to offsite power requirements, it did not seem appropriate to limit this criterion. After considering all of the comments, the SDT chose not change the wording of criterion 1.11.

Criterion 1.12 defines as Critical Assets "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection

Reliability Operating Limits (IROLs)." Comments similar to those for criterion 1.8 concerning IROLs were received on this criterion. Based on the comments received, this criterion has been reworded to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed."

Criterion 1.13 defines as Critical Assets "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes." Some commenters stated that the wording of this criterion will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. Still others stated that this criterion should use the same "bright-line" as generation, 1500 MW. This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. Based on the comments received, this criterion has been reworded to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Criterion 1.14 defines as Critical Assets "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." No commenter stated that this criterion was inappropriate for Reliability Coordinators. Several commenters stated that the term "control center" needs to be defined in the NERC Glossary. At this time, the SDT is choosing not to add control center to the NERC Glossary. The team felt that defining this term under this proposed version of the standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. Many commenters stated that control centers for Balancing Authorities (BA) and Transmission Operators (TOP) need bounds. It was stated that a small BA or TOP that does not have any other Critical Assets does not need all of the Requirements in CIP-003-4 to CIP-009-4 applied to them.

After considerable discussion, it was determined by the SDT that these "small" BAs and TOPs could be addressed in the next version of the standard. Based on the comments received, this criterion has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion 1.16 (the posted criterion 1.16 has been removed, see explanation below) has been added which states "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion 1.17 has been added which states "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

Criterion 1.15 defines as Critical Assets "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Comments received on this criterion were similar to those received on criterion 1.1 and criterion 1.14. Based on the comments received, this criterion has been reworded to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MWs in a single Interconnection."

Criterion 1.16 defines as Critical Assets "Any additional assets that the Responsible Entity deems appropriate to include." This criterion was placed in Attachment 1 to provide Responsible Entities the flexibility to include addition items on their Critical Asset list that did not meet any other

criterion in Attachment 1. Many commenters stated that this was contrary to providing a bright-line for Critical Asset identification. In addition, it has the potential of causing issues in compliance audits. For these reasons, criterion 1.16 in its current form was deleted from Attachment 1.

Question 3: Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1?

The majority of commenters that disagreed with Requirement R1 suggested changes to the wording that is present in the existing CIP-002-3. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology mentioned exists in the existing CIP-002-3 standard. The SDT expects the phraseology to be resolved in the next version. Others stated that their objection was with the wording in Attachment 1. The SDT directed them to the responses offered to their comments in question 2.

Question 4: Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2?

Of commenters that disagreed with Requirement R2, the majority suggested changes to the wording that is present in the existing CIP-002-3. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology mentioned exists in the existing CIP-002-3 standard. The SDT expects the phraseology to be resolved in the next version. Some commenters had questions about the 15-minute qualifier. The SDT's response is that this phrase is inserted to limit the scope to "real-time" operations, which is not a NERC defined term. Several commenters had suggested wording to clarify the requirement. Based on the comments received, Requirement R2 has been reworded to:

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

Question 5: Do you agree with the proposed implementation plan for the Version 4 standards?

In response to question 5, some commenters asked for new terms to be added to the NERC Glossary. At this time, the SDT is choosing not to add terms to the NERC Glossary since defining these terms would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.

APPA's review of the associated implementation plan for CIP-002-4 identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. Several entities requested that the implementation plans be combined. A NERC Standard Implementation Plan address assets that are in place and applicable the date the standard becomes effective. It is retired once the Implementation Plan is completed. The Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities addresses assets that are identified in the future and future Registered Entities and is an ongoing plan that has no expected retirement date.

Some entities asked for a provision for extensions to the implementation plan for good cause. The suggested modification proposes an exception process to a mandatory standard, and the SDT refers the entities to the discussion on technical feasibility exceptions in the FERC Order. Specifically, the oversight framework which must be in place is summarized in paragraph 222.

Some commenters felt the implementation plan was too aggressive. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Some entities requested a 24-month implementation after the effective date of the standard, and indicated that the proposed plan too complicated. The SDT has simplified the implementation plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.

Question 6: Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities?

In response to question 6, some commenters noted conforming changes that needed to be made in the implementation plan for newly identified CCAs and Responsible Entities. The SDT made these changes and will post them in the next ballot. Most other comments were similar to those offered in question 5, for which the SDT offered the same responses.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

Voter	Entity	Segment	Vote	Comment
Kirit S. Shah	Ameren Services	1	Negative	1. (a) The proposed bright line criteria are not based on any studies or performance testing. (b) The proposed bright line criteria do not address proximity to load centers or the impact to system flows or voltages in those load centers. (c)Also, we believe that impact on the BES should be evaluated for the Critical Asset using the performance requirement contained in the existing mandatory standards. This would provide consistency between CIP-002 and other standards. In this regard, we suggest that for the facilities identified in the bright line criteria, perform powerflow and stability simulations to assess the impact to the BPS of the outage of these facilities, similar to the tests performed for TPL-003 and 004. If there is an impact (that is not meeting the performance criteria), then the facility is to be considered as critical. If there is no such impact, then the facility is not be considered as critical. If there is a concern for a multi-prong attack, then similar reliability assessment should be performed for such scenarios. (d)Further, the bright line criteria will include many more facilities as critical assets with minimal to no improvement to reliability and would require significant resource commitment to meet the proposed implementation schedule. 2. We offer some comments/suggestions and also have some questions/comments to the bright line criteria (Attaachment 1): (a) The term “Facilities” should be changed to “substations and switchyards” throughout Attachment 1 as NERC glossary of terms include “lines” in the definition also. Is it SDT’s intention to include hundreds of miles of lines as critical asset? (b) The term “single station location” and “single plant location” used throughout Attachment 1 need to be defined to avoid confusion whether a single location mean one building or several buildings or stations within a defined geographical boundary or a fenced area. (c) Specific comments to Attachment 1 : 1.1 - Are there any reliability impact studies to support 1500 MW? We believe that several events larger than this number have occurred and the BES has performed as designed,

[1] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Voter	Entity	Segment	Vote	Comment
				without any loss of load, or significant impact on reliability. 1.6 - We disagree that all transmission facilities operated at 500 kV or greater are "critical". Again, system studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.7 - We disagree that all transmission facilities that are operated at 300 kV or above and are interconnected with three or more transmission substations are "critical. System studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.8 - Wording for this criterion should be changed to "Transmission substations and switchyards that the Planning Coordinator or Transmission Planner designates that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL). This change would make this criterion consist with FAC-010/FAC-014. 1.12 - We believe that the criterion reads ok, but the rationale document for this criterion implies that purpose of SPS/RAS is to prevent disturbance that would result in excursion beyond IROLs. This may not be true in all cases. 1.13 - Wording for this criterion should be changed to "Common control system(s) capable of performing automatic load shedding of 300 MW or more with a single operation". 1.15 - Same comments as for 1.1 above. 1.16 - Wording for this criterion should be changed to "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include." 3. CIP-002-4, R2 : (a) The word "associated" could mean anything to do with a Critical Assets which is too broad of a term and needs to be defined to avoid confusion. (b)The phrase "could adversely impact the reliable operation" is unclear and vague. What magnitude of "adverse impact" should be considered? Also what is being defined as the Reliable Operation? This phrase should be more clearly defined, otherwise it could introduce different interpretations in the compliance audits. 4. The implementation plan is very confusing.

Response: Thank you for your comments.

(1) The SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. Significant feedback from the industry indicated the need to simplify the Critical Asset identification approach. We welcome your suggestions for improvement to the criteria. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The results of the recent NERC data request were used to assist the team in developing the criteria in Attachment

Voter	Entity	Segment	Vote	Comment
1. Bright-line criteria by its very nature may overreach in some areas and under-reach in others, with the end result being a more protected system on average. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. (2) a) A Transmission Line can be considered a Critical Asset if it meets the criteria in Attachment 1. It would then be evaluated for possible Critical Cyber Assets, which would be afforded the cyber security protection outlined in CIP-003 to CIP-009. It is not the Critical Asset that falls under CIP-003 to CIP-009, but the Critical Cyber Asset. b) The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant. c) Item 1.1 - In prior versions we had wording about reserve sharing for the threshold. We received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. We did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Items 1.6 and 1.7 – You propose to add the criteria that the Responsible Entity can determine through a risk-based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.15 –In the development of this criterion, the drafting team used 1500 MW as a bright-line for aggregate generation controlled based on				

Voter	Entity	Segment	Vote	Comment
the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections. Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. (3) The phrase "associated" exists in the existing CIP-002-3 standard. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phrase "adversely impact" limits the scope of the evaluation of Critical Cyber Assets to those that can affect the reliable operation of 1500MW or more of generation at a single plant location. (4) The implementation plan is a modification of the implementation plan for version 3 of the CIP standards.				
Paul B. Johnson	American Electric Power	1	Negative	Overall, AEP is supportive of the efforts and the general concepts of this draft; however, there are a few refinements that will enhance the requirements and remove ambiguity. AEP encourages the SDT to consider the items below in a future draft of the standard: AEP would contend that there are regional differences that would be relevant to determine a MW threshold for generators. We support the concept that was contained in the last draft that made the determination based on the capacity reserves. However, the prior language would need to be revisited to ensure that value was fixed for a period of time. In addition, requirement 2.2 uses the term control center (also used in attachment 1) that is not a NERC defined term. This will introduce ambiguity to implementation. There has been ongoing confusion regarding the difference between "control centers" and "control rooms." We do not believe that a "control room" at a power plant or a substation would be considered a "control center." There is language in the NERC Security Guideline for Electricity Sector: Identifying Critical Assets document that the SDT should consider and incorporate into the NERC Glossary. Net real power capability testing is defined in MOD-024 standards that have yet to be FERC approved. Furthermore, not all of the regions have defined the parameters for the capability testing.
Response: Thank you for your comments. Item 1.1 - In prior versions we had wording about reserve sharing for the threshold. We received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. We did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards				

Voter	Entity	Segment	Vote	Comment
already in effect. CIP-002-4 does not require net real power capability testing.				
John Bussman	Associated Electric Cooperative, Inc.	1	Negative	Please review the submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Gordon Rawlings	BC Transmission Corporation	1	Negative	Critical Assets List comments 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations The present wording uses an arbitrary numbers of stations, the number of stations is immaterial BCH recommends the "Transmission Facilities operated at 300 kV or higher that if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. A clear definition of common control system(s) is required. Is under frequency or under voltage load shedding schemes considered control systems? The load shedding of 300 MW or more does it include firm or interruptible load or both? 1.16. Any additional assets that the Responsible Entity deems appropriate to include. To encourage reliability the additional assets deemed appropriate by a Responsible Entity should not be auditable.
Response: Thank you for your comments. Item 1.7 – In order to be more accurate in terms of the impact, the drafting team thought that it was more appropriate to refer to the number of connected transmission substations instead of using IROLs. The intent was to avoid double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them. This includes upstream, downstream, radial and networked substations. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.				

Voter	Entity	Segment	Vote	Comment
Joseph S. Stonecipher	Beaches Energy Services	1	Negative	See my comments in the survey on the NERC Website for Cyber Security 706.
Response: Thank you for your comments. Please refer to the response to comments document.				
Donald S. Watkins	Bonneville Power Administration	1	Negative	Please refer to BPA comments submitted during the formal comment period on 10/26/10.
Response: Thank you for your comments. Please refer to the response to comments document.				
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	See response submitted on the Comments Form.
Response: Thank you for your comments. Please refer to the response to comments document.				
Paul Rocha	CenterPoint Energy	1	Negative	CenterPoint Energy appreciates the work of the SDT and feels that the proposed Standard is very close. As stated in comments previously submitted, CenterPoint Energy belives criteria 1.11 in Attachment 1 is unnecessary and should be deleted or, if the SDT feels some criteria regarding nuclear facilities is needed then it should be limited to transmission facilities that directly connect the nuclear generator output to the transmission system. With either of these two changes CenterPoint Energy beleives it could support the proposed Standard.
Response: Thank you for your comments. Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2, "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets.				
Michael B Bax	Central Electric Power Cooperative	1	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Jack Stamper	Clark Public Utilities	1	Negative	Attachment 1, part 1.14 would make a control centers performing the functional obligation of a TOP a Critical Asset. This apparently would be the case even if a TOP's control center only performed these functions on facilities that are not critical. Small entities have in some cases been forced by Balancing Authorities and former Transmission Operators to register as TOPs. Many of these TOPs operate systems with no assets that qualify as Critical Assets under any of the other Attachment 1 criterion. Some of these TOPs operate systems that do not have any Bulk Electric System facilities. It is unreasonable to designate these utilities dispatch centers as Critical Assets. Part 1.14 should be modified as follows: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator over any facilities determined to be Critical Assets as determined in Attachment 1, criterion 1.1 through 1.13.
Response: Thank you for your comments. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
John K Loftis	Dominion Virginia Power	1	Negative	Dominion conceptually supports bright line criteria for determining critical assets. However, we cannot vote in favor at this time because we believe that changes are needed in Table 2 that recognize the implementation for infrastructure (physical and electronic security) should be equal to, or longer than, that required for training. We also believe that the bright line criteria for generation control center needs further effort. Please see more specific comments/recommendations submitted by Dominion.
Response: Thank you for your comments. Please refer to the response to comments document.				
George S. Carruba	East Kentucky Power Coop.	1	Negative	EKPC would suggest rewording R2 to say: "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those interconnected Cyber Assets that collectively could adversely

Voter	Entity	Segment	Vote	Comment
				impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes."
Response: Thank you for your comments. Requirement R2 has been changed based on industry comments received.				
Ralph Frederick Meyer	Empire District Electric Co.	1	Negative	EDE understand that NERC standards are a minimum requirement and regions can look at their own operating criteria and determine if they need additional protection at lower Megawatt bright-lines. EDE agrees with APPA in that they are concerned that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we agree that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2. EDE agrees with Cleco in that there is a dichotomy between 1.1. that states generation "equal to or exceeding 1500 MW" and 1.15. that states control centers that control generation "greater than an aggregate of 1500 MWs" There should be consistency between the two. EDE agrees with AAPA in that:APPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: "Adverse Reliability Impacts" will help clarify which units should be in this category. We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. APPA proposes the following rewording of criteria 1.3: 1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer. EDE agrees with AAPA in that Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan's overall effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset. EDE agrees with LES in that this language should be changed to "Each Blackstart Resource identified in the Transmission Operator's restoration plan as used to directly start

Voter	Entity	Segment	Vote	Comment
				generation identified as a Critical Asset, or identified in the Transmission Operator's restoration plan as used to directly start generation greater than an aggregate of 300 MW." 1.5 EDE does request clarification of criteria 1.5: Where does this point of multiple paths lay in the electrical system? Does this include only the Generator Step-up Transformer, or does it include the whole substation where multiple transmission paths depart to a single generator? EDE believes that criteria 1.8 and 1.9 should be reworded to "station or substation" instead of just "station" so that it is not implied that it only applies to power plants (station). EDE seeks verification from the SDT that the SPS they refer to in criteria 1.12 is for wide area protection only. EDE agrees with APPA suggested change in 1.13: 1.13. Common control system(s) configured to perform automatic load shedding of 300 MW or more within 15 minutes. EDE agrees with APPA in that we can accept the bright-line of 300 MW if the wording is changed to that stated above, but we still see this bright-line as an arbitrary threshold based on a quantity that has no BES operational significance. Rather, 300 MW is a DOE threshold for electric event reporting. EDE agrees with APPA in that criteria 1.14. is overly broad because it includes all BA and TOP control centers regardless of size. EDE asks that the SDT revise this criteria to include a bright-line with similar impact as those in 1.1 and 1.15. EDE agrees with APPA revised wording: 1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator with a minimum of 1500 MW of resources under its control. EDE agrees with AAPA in that we cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability or uncontrolled separation of the BES. However, we will support inclusion of "ALL BA and TOP control centers" only when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal. In the NERC Draft CIP-002-4 webinar it was stated that a control center in criteria 1.15 is understood to be controlling multiple units. EDE agrees with APPA recommendation that the SDT clarify the wording in criteria 1.15 to coincide with this understanding: 1.15. Each control center or backup control center used to control multiple generation units identified as Critical

Voter	Entity	Segment	Vote	Comment
				Assets designated under criterion 1.3 or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. EDE agrees with AAPA in that 1.16 should be removed from the Attachment 1 criteria. We expect that registered entities may voluntarily protect assets above and beyond the ones listed in these criteria. However, we just do not see the reliability benefit of imposing a compliance liability to those self identified critical assets. We feel that the NERC and Regional compliance staff will waste valuable time and resources evaluating entity compliance with cyber security controls for assets that are outside of the scope of this standard For newly identified Critical Assets, a 24 month implementation is provided for Entities that have never identified a Critical Asset under the version 3 standards, with only 18 months provided for Entities with existing Critical Assets. We believe the SDT has developed a sound approach with this delineation. However, we also believe the 24 month implementation should be expanded to include Entities that may have existing Critical Assets, but have never identified a Critical Asset of a given type, i.e., generating unit, transmission facility, control center, etc. For example, if a company had a control center that was previously identified as critical, but version 4 results in their first generating unit being identified, then we would propose that they be given 24 months to become compliant as they are working on their first generating unit. EDE agrees with AAPA in that a review of the associated Implementation Plan for CIP-002-4 has identified a potential inconsistency between the Implementation Plan and the Reliability Standard. The Reliability Standard clearly provides that updates to the Critical Asset list will be made at the time of the annual review. However, the Implementation Plan is not as clear. We would request modification to the Implementation Plan such that it reflects the intent of the Reliability Standard. The Implementation Plan does not adequately address when a “New Asset” that does meet the CIP-002-4 criteria for being a Critical Asset after its commissioning will need to be in compliance. EDE agrees with APPA in that the intent of the Reliability Standard indicates that the post-commissioned New Asset will become a Newly Identified Critical Asset upon the subsequent Annual Review and only at the time of this Annual Review. Further that the timeline associated with this Newly Identified Critical Asset starts with the date of the Annual Review. We raise this point because we are concerned about the potential impact for confusion associated with multiple review dates or continuous reviews of the assets contained within numerous CIP activities. If an entity

Voter	Entity	Segment	Vote	Comment
				has multiple Cyber Assets, the entity would likely have multiple Annual Reviews dates.

Response: Thank you for your comments.

Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12-month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright-line. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.
Criterion 1.15 has been modified to conform to the MW wording in 1.1.

Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize.

Items 1.8 & 1.9 - The SDT changed "stations" to "stations or substations."

Item 1.12 – Since this item only applies to SPSs that have IROLs associated with them, local area SPSs are not included.

Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset

Voter	Entity	Segment	Vote	Comment
identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. Implementation Plan issues - Thank you for your comments. Requirements R1 and R2 were modified to clarify that the update is ongoing, and the review must occur at least annually. The text reference was removed from the Implementation Plan.				
George R. Bartlett	Entergy Corporation	1	Negative	Switchyards serving nuclear facilities should not be automatically classified as critical assets. - The fact that a BES switchyard serves a nuclear facility should not in itself qualify the switchyard as a critical asset. While nuclear units and their support facilities may qualify as critical assets under a separate set of criteria, they should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability. All blackstart units and associated cranking paths should not be automatically classified as critical assets. - Blackstart units may be useful in the restoration of the BES following a large scale outage, but they are not necessarily essential to the reliability of the BES under normal operation. Blackstart units should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability.
Response: Thank you for your comments. Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2, "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.				

Voter	Entity	Segment	Vote	Comment
Dennis Minton	Florida Keys Electric Cooperative Assoc.	1	Negative	Cost prohibitive for small entities that have little to no material impact to the BES.
Response: Thank you for your comments. Cost is only one of many issues that must be considered in the cyber security of the BES.				
Gordon Pietsch	Great River Energy	1	Negative	GRE commented during the comment period and the drafting team should refer to those comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Ajay Garg	Hydro One Networks, Inc.	1	Negative	Hydro One is casting a negative vote for the following reasons: 1. We do not believe the standard will result in an improvement in reliability since the revisions merely replace the risk-based assessment methodology with a list of criteria that will ultimately result in inclusion of facilities on the Critical Assets list that are non-impactive on the BES. 2. We do not agree with criteria 1.6 and 1.7 in Attachment 1 as written. Application of these criteria would result in the inclusion of facilities that will have no impact on the BES reliability. We believe that the list of applicable facilities should be determined following an impact-based assessment to be performed by the Reliability Coordinator. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct/review the assessment should be included. We therefore propose the following wording to replace 1.6 and 1.7 in Attachment 1: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission Facilities operated at 300 kV or higher to less than 500 kV at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages. 3. We do not agree with the removal of the exclusion that applies to facilities regulated by the Canadian Nuclear Safety Commission from the Applicability Section, This explicit statement makes it clear that CIP standards do not apply to those facilities

Voter	Entity	Segment	Vote	Comment
				which would not be the case if it were removed.
Response: Thank you for your comments. 1) The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology. 2) Items 1.6 and 1.7 – The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. 3) The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
Bernard Pelletier	Hydro-Quebec TransEnergie	1	Negative	1- CIP-002-4, Attachment 1, as posted, is a simple list of assets that appears without mention of any performance based requirement. We believe that to be an effort to "cast a wider net" and capture more assets without qualifying their actual criticality. Attachment 1 inclusion criteria for critical assets should be based on critical functions of assets like: system restoration, voltage control, maintaining load/generation balance, maintaining flows within IROL/SOL, critical SPS. This list should not rely on substation voltages or amount of MW. 2- Also, the term "group of generating unit" in CIP-002-4, R2 and 1.1 of Attachment 1 is not clear. Does it mean a generating station? A group of units sharing the same transformer? 3- The 15 minutes delay of reliable operation referred in CIP-002-4, R2 is not clear too. How it will be determine that operations are not reliable after 15 minutes? Does this 15 minutes period is the Disturbance Recovery Period referred in BAL-002 Reliability Standard? 4- Hydro-QuÃ©bec does not agree with the removal of item (4.2.1) from the revised CIP002-4. We consider that the Canadian Nuclear Safety Commission should still be exempted from the standard CIP-002. 5- The cross references are still part of some CIP and it's sometimes makes the interpretation of the requirements more complex. For example CIP-007-4 R5.1.3 "Account Management" indicates the review should be done annually in accordance with CIP-004-4 E4 but the R4.1 indicates the review should be done quarterly. A table that explains the different requirements instead of a cross reference would be more useful.
Response: Thank you for your comments. 1) The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology.				

Voter	Entity	Segment	Vote	Comment
2) Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant. 3) The reference to 15 minutes was inserted to keep the scope to "real-time" operations, an undefined term. 4) The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
Walter Kenyon	KAMO Electric Cooperative	1	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Stan T. Rzad	Keys Energy Services	1	Negative	The SDT is commended on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				
Larry E Watt	Lakeland Electric	1	Negative	LAK cannot support this standard revision without some form of bright line cutoff to exclude small BAs and TOPs that cannot cause instability, cascading or uncontrolled separation of the BES.
Response: Thank you for your comments. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
John W Delucca	Lee County Electric Cooperative	1	Negative	General Comments & Information Security Best Practices NERC distributed a questionnaire to responsible entities to gauge the impact of the proposed changes to CIP-002-4. The bright line criteria has changed since this

Voter	Entity	Segment	Vote	Comment
				assessment was performed and will result in the inclusion of additional assets being categorized as Critical Assets. Existing studies prove that many of these assets are not Critical Assets and do not impact the reliability of the BES. The existing CIP3 - CIP9 standards are not being modified with the version four release even though there are many opportunities to improve these standards. A good example can be seen with the Technical Feasibility Exception (TFE) process. Why are entities and regulatory agencies being forced to spend a significant amount of time processing TFE's because requirements don't make sense? A good example is the common TFE for routers and switches that do not and cannot run antivirus software. Expanding the scope of these labor intensive and non-value added processes will only deter entities from implementing effective security measures and best practices. A prudent approach would be to adjust the bright line criteria to ensure that the assets being included in the scope of the version four standards are truly Critical Assets. Once the security control standards are improved, the scope can be expanded to include medium and low impact cyber systems. Attachment 1 & Criteria Suggestions Attachment 1: o Paragraph 1.14 includes the Transmission Operator (TOP) function in addition to the Reliability Coordinator (RC) and Balancing Authority (BA) functions. In CIP10 the concept of a true "risk based" approach to the application of security requirements was proposed in the purpose section of the document as follows: Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES, for the application of cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES. The concept of matching security controls with risk is common practice that is found in NIST and ISO guidelines for risk management. These best practices should be leveraged when considering the implementation of CIPv4 and the development of future standards such as CIP10 and CIP11 that will include requirements for medium and low risk BES Cyber Systems. In the draft release of CIP10, the Balancing Authority (BA), Reliability Coordinator (RC) and Transmission Operator (TOP) functions were listed separately and with additional qualifying criteria. This is a much better approach that is well aligned with best practices and future standard development. When considering the proposed CIPv4 criteria, the control centers for the Transmission Operator (TOP) function should only be included as Critical Assets if they operate transmission facilities that meet the critical asset

Voter	Entity	Segment	Vote	Comment
				bright line criteria listed in paragraph 1.6 (above 500kV) or 1.7 (300Kv or higher at stations interconnected at 300kV or higher with three or more other transmission stations). Not including these criteria will cause Non-Critical Assets to be identified as Critical Assets. In addition, the standards will go against established best practices and be in conflict with the already released draft of the CIP10 and CIP11 standards. Suggested change to Attachment 1 paragraph 1.14: Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator or Balancing Authority. Suggested change to Attachment 1 (Add paragraph 1.x): Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Transmission Operator for Transmission Facilities meeting the criteria in 1.6 or 1.7. Requirement R2 Comments This section of R2 makes the requirement very confusing: For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. If this is intended to be further clarification for generating units only, there should be a paragraph for this alone. In addition, the basis for "within 15 minutes" is not defined and could lead to subjectivity in the interpretation of this requirement.

Response: Thank you for your comments.

The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1. The 15-minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential

Voter	Entity	Segment	Vote	Comment
after a longer period of time but do not necessarily involve real-time reliability impact. We have updated the wording of R2 to clarify the meaning of this phrase.				
William Price	M & A Electric Power Cooperative	1	Negative	Please review my submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Michelle Rheault	Manitoba Hydro	1	Negative	Please see comments submitted by Manitoba Hydro in the formal comment period.
Response: Thank you for your comments. Please refer to the response to comments document.				
Danny Dees	MEAG Power	1	Negative	MEAG supports the APPA's comments submitted to the NERC CIP standard drafting team.
Response: Thank you for your comments. Please refer to the response to comments document.				
Randi Woodward	Minnesota Power, Inc.	1	Negative	Please see comments submitted during the Comment Period.
Response: Thank you for your comments. Please refer to the response to comments document.				
Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Richard L. Koch	Nebraska Public Power District	1	Negative	NPPD agrees with and supports the comments provided by the American Public Power Association (APPA).

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Kevin White	Northeast Missouri Electric Power Cooperative	1	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Robert Mattey	Ohio Valley Electric Corp.	1	Negative	Technical justification for "Bright line" criteria lacking.
Response: Thank you for your comments. The SDT believes information provided in the posted guidance document provides sufficient technical justification for each criterion.				
Brad Chase	Orlando Utilities Commission	1	Negative	SDT Proposed: 1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. APPA Comments: APPA and others commented on the CIP-010-1 standard as having arbitrary bright lines for generating units and requested that these bright line numbers have justification or have them based on the Contingency Reserve of each Reserve Sharing Group region. APPA commends the SDT for their attempted to come to agreement on a nationwide bright line for generating units based on an operationally significant threshold. The use of an average of the Contingency Reserve numbers from all the regions bases the bright-line on what the regions consider operationally significant. We understand that NERC standards are a minimum requirement and regions can look at their own operating criteria and determine if they need additional protection at lower Megawatt bright-lines. APPA is concerned that the use of the “Real Power Capability of the preceding 12 months” would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. To alleviate this volatility we suggest that generation owners should use the facility ratings which are calculated and communicated under FAC-009-1 R2. R2. The Transmission Owner and Generator Owner shall each provide Facility Ratings for its solely and jointly owned Facilities that are existing Facilities, new Facilities, modifications to existing Facilities and re-ratings of existing Facilities to its associated Reliability Coordinator(s), Planning

Voter	Entity	Segment	Vote	Comment
				Authority(ies), Transmission Planner(s), and Transmission Operator(s) as scheduled by such requesting entities. SDT Proposed: 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. APPA Comments: APPA does not have a comment on criteria 1.2 at this time. SDT Proposed: 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes. APPA Comments: APPA commends the SDT on including the criteria in 1.3, which gives the PC and TP the ability to designate as critical any generating facilities for reliability purposes. This will cover critical units that are not captured within the bright line of criteria 1.1 without drawing in all units of a certain size that are not considered critical elsewhere on the system. APPA suggests that the designation of facilities be based on studies conducted under the TPL standards to justify the designation. Also, the use of NERC Glossary of term: “Adverse Reliability Impacts” will help clarify which units should be in this category. We are also concerned that the PC or TP will be looking at local vs. wide area reliability. There are some cases where the PC can designate Must Run units for temporary situations so this must be clarified within the criteria. APPA proposes the following rewording of criteria 1.3: “1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required to avoid BES Adverse Reliability Impacts for 1 year or longer.” SDT Proposed: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. APPA Comments: APPA is concerned that designating all Blackstart Resources as critical will divert limited resources to protect blackstart facilities that are only used to restore localized load. We believe it is the intent of the drafting team to identify the truly critical blackstart units (taking from the CIP-010-1 draft; only high impact facilities). APPA understands that criteria 1.4 uniformly identify all Blackstart Resources listed in the Transmission Operator’s restoration plan as being Critical Assets with regards to the Bulk Electric System. Currently, many utilities include multiple Blackstart resources in the restoration plans provided to the Transmission Operator. Including numerous resources makes the plan much more robust and reliable as it provides additional well documented restoration options should unforeseen problems occur. As currently written, Item 1.4 inadvertently incentivizes utilities to remove blackstart resources from the restoration plan if these resources are not critical to an effective regional restoration plan, reducing the plan’s overall

Voter	Entity	Segment	Vote	Comment
				effectiveness. Therefore, we believe there should be a threshold for Blackstart Resources, similar to nearly all other elements being considered in Attachment 1. This would allow utilities the freedom to include numerous resources in the Transmission Operators restoration plan without being swept into being identified as a critical asset. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. For example, a 10 MW Blackstart Resource that directly supports restoration of a critical generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies local load during an outage. Therefore, APPA would propose judging the criticality of a Blackstart Resource by the relative importance of the generating unit(s) it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of criteria 1.15 and the capacity bright-line of criteria 1.13: 1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan, which meet either of the following criteria: 1.4.1 Used to directly start generation identified as a Critical Asset in criteria 1.1 or 1.3, 1.4.2 Used to directly start generation greater than an aggregate of 300 MW. We believe this approach should provide a better measure of a Blackstart Resource's potential impact on the Bulk Electric System, resulting in Critical Assets that adequately address system reliability in a practical manner. It also mitigates the likelihood that registered entities may decide to retire certain small blackstart units, thereby removing valuable but not critical blackstart resources from the Transmission Operator's restoration plan. We further support inclusion of "ALL Blackstart Resources" only when this standard is revised to provide for a tiered (High, Medium and Low) categorization of Critical Assets, such as the SDT's draft CIP-010-1 proposal. SDT Proposed: 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. APPA Comments: APPA commends the SDT on differentiating between a single Cranking Path as a critical facility and multiple Cranking Paths as having redundancy in the BES and thus being less critical. Having this criteria stated in 1.5 incentivizes the entity to build in redundancy in infrastructure to lower criticality of a single asset. This truly does reward infrastructure reliability through a standard. APPA does request clarification of criteria 1.5: Where does this point of multiple paths lay in the electrical system?

Voter	Entity	Segment	Vote	Comment
				Does this include only the Generator Step-up Transformer, or does it include the whole substation where multiple transmission paths depart to a single generator? Also, APPA suggests that the SDT change "switching requirements" to "switching equipment." SDT Proposed: 1.6. Transmission Facilities operated at 500 kV or higher. APPA Comments: APPA does not have a comment on criteria 1.6 at this time. SDT Proposed: 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. APPA Comments: APPA bel
Response: Thank you for your comments. Item 1.1 – The SDT notes your concern that the use of the "Real Power Capability of the preceding 12 months" would bring in unnecessary volatility to applicability of this standard to certain groups of generating units. The drafting team used time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used. The 12-month time period was used so that seasonal ratings would not be an issue for generating plants that operate near the 1500 MW bright-line. Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize.				
Richard J Kafka	Potomac Electric Power Co.	1	Negative	Pepco Holdings has submitted comments in the names of its affiliates, including Potomac Electric. Pepco would consider an affirmative vote if these issues are addressed.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Laurie Williams	Public Service Company of New Mexico	1	Negative	PNM Resources applauds the significant effort of the SDT in developing the revision to CIP-002-4, and conforming changes to CIP-003-4 through CIP-009-4. Although the most recent version of CIP-002-4 represents significant progress, PNM Resources must cast a negative vote with the following comments: The criteria related to blackstart resources do not consider the varying role of blackstart resources identified in restoration plans, and, as drafted, will require identification of any blackstart resource, or path, mentioned in a restoration plan to be identified as a Critical Asset. Entities in many regions may identify a significant number of Blackstart Resources in a restoration plan, representing primary and alternate resources allowing for a number of options for system restoration. PNM Resources recommends the following revisions to the criteria: 1.4. Each primary Blackstart Resource essential to the Transmission Operator's restoration plan. 1.5. The Facilities comprising the primary Cranking Paths and initial switching requirements from the primary Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.
Response: Thank you for your comments. Items 1.4 and 1.5 – The SDT considered using the word "primary," but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.				
Kenneth D. Brown	Public Service Electric and Gas Co.	1	Negative	Please see PSEG Companies' comments filed separately. The PSEG companies will change the vote to affirmative if the comments are adequately addressed by the drafting team.
Response: Thank you for your comments. Please refer to the response to comments document.				
Catherine Koch	Puget Sound Energy, Inc.	1	Negative	PSE supports this revision, however feels further clarity is necessary regarding Attachment 1, section 1.1, to recognize that a generation plant that is tripped as part of a Remedial Action Scheme (Special Protection System) in place to protect the Bulk Electric System should be exempted

Voter	Entity	Segment	Vote	Comment
				from Critical Asset designation. The inclusion of a generation plant in a RAS scheme infers that the plant is not critical to the operation of the BES. NERC included this same criteria in their guidance document "Security Guideline for the Electricity Sector: Identifying Critical Assets," page 10, table C-2.
Response: Thank you for your comments. Criterion 1.1 is based on plant size. Criterion 1.12 stipulates Facilities related to SPSs and RASs. Both criteria should be used to determine whether a generation plant qualifies as a Critical Asset.				
Tim Kelley	Sacramento Municipal Utility District	1	Negative	After reviewing the proposed version 4 language for CIP-002, R2, the placement of the additional text on generation is confusing. It appears to be trying to accomplish two different purposes. SMUD does not have any objections to the text itself, just the placement. SMUD proposes organizing the requirement as follows: R2. Critical Cyber Asset Identification- Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall review this list at least annually, and update it as necessary. R2.1 For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.1.2 The Cyber Asset uses a routable protocol within a control center; or, R2.1.3 The Cyber Asset is dial-up accessible. R2.2 For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1., the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Additionally, SMUD, as a member of APPA, would like to reflect its support to those CIP-002-4 Standard comments submitted by APPA staff.
Response: Thank you for your comments. Please refer to the response to comments document for responses to APPA comments. Requirement R2 has been changed to clarify the issues presented.				
Robert Kondziolka	Salt River Project	1	Negative	SRP believes that a bright line assessment methodology for determining Critical Assets is not in the best interest of reliability. This is especially true in the designation of substations and generating facilities. The attributes of these stations and their unique impact on Bulk Electric System reliability

Voter	Entity	Segment	Vote	Comment
				must be taken into account. There are several terms and phrases used within Requirement 2 of the proposed Standard that need to be better defined to eliminate ambiguity. These terms are: 1) essential to the operation of the Critical Asset, 2) adversely impact the reliable operation needs to be defined; and, 3) within 15 minutes. We believe the CIP-002-4 implementation plan for newly identified Critical Assets and associated Critical Cyber Assets provides inadequate time. SRP suggests the implementation timeframe be extended to 30 months after the effective date of the Standard.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about (annual) exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Denise Stevens	Sho-Me Power Electric Cooperative	1	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Rich Salgo	Sierra Pacific Power Co.	1	Negative	This is a negative vote due solely to disagreement over some of the elements in Attachment 1 of the Standard. Overall, the draft Standard promotes the necessary clarity over which Assets shall be Critical. Detail comments have been provided via the official comment response form. In general, we believe that Attachment 1 is overly inclusive of elements and facilities that may have no material impact on BES reliability. In particular, we believe that not all blackstart resources should be treated identically - perhaps only the primary blackstart resource of a TOP's restoration plan should be identified; the designation of a facility as "required for reliability purposes" by a Planning entity needs more precision and clarification that this shoudl be limited to those facilities that have a perpetual reliability need, not an occasional one; 300kV and higher facilities ought not to be

Voter	Entity	Segment	Vote	Comment
				included unless they connect to four or more non-radial 300kV+ stations; and need further clarification of the distinction between generation control rooms and control centers.
Response: Thank you for your comments. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection."				
Horace Stephen Williamson	Southern Company Services, Inc.	1	Negative	Comments were submitted via Comment Form: Project 2008-06 - Cyber Security 706
Response: Thank you for your comments. Please refer to the response to comments document.				
William G. Hutchison	Southern Illinois Power Coop.	1	Negative	I realize that the politically correct want all BES assets to have some level of criticality, but the truth still remains that there are assets on the BES that are not critical to the operation of the BES. This is another prime example of creating compliance standards that only create documentation compliance and do not provide performance based standards.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method.				

Voter	Entity	Segment	Vote	Comment
Larry Akens	Tennessee Valley Authority	1	Negative	Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this CIP-002-4 draft. We fully support the standards development process and all the hard work and commitment by the drafting team members. For this draft, we have the following concerns which moved us to cast a Negative vote. Comments: Q1: Yes; no comment Q2: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. The language appears to require us to designate "Each" component in the System Restoration plan as CA. We currently include at least 2 paths for black start of every generation plant in the system, which would extend CA designation to a large number of components which otherwise would not be included by other criteria. The flexibility provided by our robust transmission infrastructure and large number black start capable plants serves to help ensure reliable operation of the BES, but designating as a CA each component that could participate in the total paths possible doesn't seem consistent with the intent of the standard. Recommendation: Revise language to allow entities to limit CA designation to those components participating in the primary black start path. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3. There isn't a clear definition of the term "directly connected." Without this definition there are many way to interpret this requirement. Is this language meant to describe a facility where the substation is co-located with a generation facility? Also, does the language this mean total loss of substation or only partial? Recommendation: For the purpose of this standard revise language to clearly define "directly connected." Q3: Yes; no comment Q4: Yes; no comment Q5: abstain Q6: abstain

Response: Thank you for your comments.

Item 1.4 – The SDT considered using the word "primary," but ultimately rejected it as it is not a defined NERC Glossary term, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Voter	Entity	Segment	Vote	Comment
Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any transmission Facility that, if lost, would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include the partial or total loss of a substation.				
James W. Beck	Transmission Agency of Northern California	1	Negative	TANC hereby submits a negative vote on this ballot and refers the project drafting team to comments submitted by the American Public Power Association.
Response: Thank you for your comments. Please refer to the response to comments document.				
Jonathan Appelbaum	United Illuminating Co.	1	Negative	Concerns with CIP-002 V4 Attachemnt 1. Comment form submitted and concurrence with EEI comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Gregory L Pieper	Xcel Energy, Inc.	1	Negative	Please see our comments submitted during the concurrent comment period.
Response: Thank you for your comments. Please refer to the response to comments document.				
Venkataramakrishnan Vinnakota	BC Hydro	2	Negative	1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations The present wording uses an arbitrary numbers of stations, the number of stations is immaterial BCH recommends the "Transmission Facilities operated at 300 kV or higher that if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. A clear definition of common control system(s) is required. Is under frequency or under voltage load shedding schemes considered control systems? The load shedding of 300 MW or more does it include firm or interruptible load or both? 1.16. Any additional assets that the Responsible Entity deems appropriate to include. To encourage reliability the additional assets deemed appropriate by a Responsible Entity should not be auditable.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Item 1.7 – In order to be more accurate in terms of the impact, the drafting team thought that it was more appropriate to refer to the number of connected transmission substations instead of using IROLs. The intent was to avoid double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them. This includes upstream, downstream, radial and networked substations. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.				
Chuck B Manning	Electric Reliability Council of Texas, Inc.	2	Negative	ERCOT ISO has joined in the submission of the IRC SRC comments. Please see IRC SRC submission for details.
Response: Thank you for your comments. Please refer to the response to comments document.				
Kim Warren	Independent Electricity System Operator	2	Negative	We repeat the main reasons for our negative vote which are also stated in our comments on this project (submitted today). We do not agree with criteria 1.6 and 1.7 as written since some of the facilities identified as Critical Assets by applying them may have no impact on the BES. We therefore believe the list of relevant transmission facilities developed by the Responsible Entity, should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. We therefore propose the following specific wording: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no

Voter	Entity	Segment	Vote	Comment
				impact outside the local area and will not cause BES instability, separation, or cascading outages. Additionally, we do not agree with the removal from the Applicability Section, of the exclusion that applies to facilities regulated by the Canadian Nuclear Safety Commission. This explicit statement makes it clear that CIP standards do not apply to those facilities which would not be the case if it were removed.
Response: Thank you for your comments. Items 1.6 and 1.7 – You propose to add the criteria that the RC can determine through a risk-based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The inclusion of a risk-based evaluation by any entity would not meet the objective of uniform application of Critical Asset identification across all entities. The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	We are concerned that criterion 1.3 in Attachment 1 of CIP-002-4 could be construed as transferring the responsibility for identifying Critical Assets from Generation Owners to the Planning Coordiantors. We oppose this and believe the obligation rests with the asset owner. Furthermore, paragraph 328 of Order 706 makes clear that the asset owner cannot transfer its responsibility for identifying Critical Assets to a third party. We suggest this criteria should be removed. Criteria 1.8, 1.9, and 1.12 should be modified because loss of facilities does not cause an IROL violation. An IROL includes a limit and a time constant Tv. In order for an IROL violation to occur, the limit must be exceeded for at least the time constant Tv. Tv is usually 30 minutes. Thus, when we consider the impact on the loss of facilities on an IROL, an operator will have enough time to adjust the system to prevent an IROL violation. For 1.8, the criterion should be modified to reflect that the facilities that comprise an IROL should be considered critical. The drafting team may also wish to consider loss of any facilities that set up the need for the IROL or cause the actual limit to change. For criterion 1.9, it is not clear why FACTs devices need to be singled out. Are they not covered in criterion 1.8 under Transmission Facilities? Inclusion of 1.9 is redundant and just causes confusion because it causes the reader to infer that the drafting team intended for them to be treated differently when in fact the criterion is the same as 1.8. For criterion 1.12, it would be more appropriate to assess the impact of an SPS, RAS, or automated switching system on the IROL. If loss of the SPS,

Voter	Entity	Segment	Vote	Comment
				RAS, or automated switching system causes an IROL to decrease, then the SPS, RAS, or automated switching system should be considered critical.
Response: Thank you for your comments. Item 1.3 – The burden for identifying Critical Assets is still the Responsible Entity that is the asset owner. There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability. This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – FACTS devices were singled out to ensure that there was no confusion as to whether or not they were considered Critical Assets. Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed."				
Richard J. Mandes	Alabama Power Company	3	Negative	Comments were submitted via Comment Form: Project 2008-06 - Cyber Security 706
Response: Thank you for your comments. Please refer to the response to comments document.				
Raj Rana	American Electric Power	3	Negative	Overall, AEP is supportive of the efforts and the general concepts of this draft; however, there are a few refinements that will enhance the requirements and remove ambiguity. AEP encourages the SDT to consider the items below in a future draft of the standard: AEP would contend that there are regional differences that would be relevant to determine a MW threshold for generators. We support the concept that was contained in the last draft that made the determination based on the capacity reserves. However, the prior language would need to be revisited to ensure that value was fixed for a period of time. In addition, requirement 2.2 uses the term control center (also used in attachment 1) that is not a NERC defined

Voter	Entity	Segment	Vote	Comment
				term. This will introduce ambiguity to implementation. There has been ongoing confusion regarding the difference between "control centers" and "control rooms." We do not believe that a "control room" at a power plant or a substation would be considered a "control center." There is language in the NERC Security Guideline for Electricity Sector: Identifying Critical Assets document that the SDT should consider and incorporate into the NERC Glossary. Net real power capability testing is defined in MOD-024 standards that have yet to be FERC approved. Furthermore, not all of the regions have defined the parameters for the capability testing.
Response: Thank you for your comments. Item 1.1 - The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. At this time, the SDT is choosing not to add "control center" to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. CIP-002-4 does not require net real power capability testing.				
Nathan Mitchell	American Public Power Association	3	Negative	See APPA CIP-002-4 Task Force Comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Chris W Bolick	Associated Electric Cooperative, Inc.	3	Negative	Please review submitted comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Pat G. Harrington	BC Hydro and Power Authority	3	Negative	Critical Assets List comments 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations The present wording uses an arbitrary numbers of stations, the number of stations is immaterial BCH recommends the "Transmission Facilities operated at 300 kV or higher that if destroyed, degraded, misused or otherwise rendered unavailable, violate

Voter	Entity	Segment	Vote	Comment
				one or more Interconnection Reliability Operating Limits (IROLs). 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. A clear definition of common control system(s) is required. Is under frequency or under voltage load shedding schemes considered control systems? The load shedding of 300 MW or more does it include firm or interruptible load or both? 1.16. Any additional assets that the Responsible Entity deems appropriate to include. To encourage reliability the additional assets deemed appropriate by a Responsible Entity should not be auditable.
Response: Thank you for your comments. Item 1.7 – In order to be more accurate in terms of the impact, the drafting team thought that it was more appropriate to refer to the number of connected transmission substations instead of using IROLs. The intent was to avoid double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them. This includes upstream, downstream, radial and networked substations. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.				
Rebecca Berdahl	Bonneville Power Administration	3	Negative	Please refer to BPA comments submitted during the formal comment period on 10/26/10
Response: Thank you for your comments. Please refer to the response to comments document.				
Ralph J Schulte	Central Electric Power Cooperative	3	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Steve Alexanderson	Central Lincoln PUD	3	Negative	Please see comments posted by Steve Alexanderson at Central Lincoln.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Linda R. Jacobson	City of Farmington	3	Negative	FEUS agrees with APPA's comments and proposed changes.
Response: Thank you for your comments. Please refer to the response to comments document.				
Gregg R Griffin	City of Green Cove Springs	3	Negative	FMPA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				
Roger Powers	City Water, Light & Power of Springfield	3	Negative	While the "bright line" approach satisfies the FERC requirement for ERO guidance in the development of Risk-based Methodology, it does not allow for the flexibility to consider each responsible entity's individual circumstances as suggested in Paragragh 253 of FERC Order 706. It is not clear that a risk assessment was used to develop the "bright lines" contained in the standard.
Response: Thank you for your comments. Regarding the directives for external review and guidance in the FERC Order, the SDT believes the criteria in Attachment 1 are in response to FERC Order 706 paragraph 329. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This "bright-line" approach removes the variability of entity defined methodologies that would prompt the need for external review.				
Russell A Noble	Cowlitz County PUD	3	Negative	Please refer to APPA's and my comments.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Michael F Gildea	Dominion Resources Services	3	Negative	Dominion conceptually supports bright line criteria for determining critical assets. However, we cannot vote in favor at this time because we believe that changes are needed in Table 2 that recognize the implementation for infrastructure (physical and electronic security) should be equal to, or longer than, that required for training. We also believe that the bright line criteria for generation control center needs further effort. Please see more specific comments/recommendation submitted by Dominion.
Response: Thank you for your comments. Please refer to the response to comments document.				
Anthony L Wilson	Georgia Power Company	3	Negative	Comments were submitted via Comment Form: Project 2008-06 - Cyber Security 706
Response: Thank you for your comments. Please refer to the response to comments document.				
Gwen S Frazier	Gulf Power Company	3	Negative	Comments were submitted via Comment Form: Project 2008-06 - Cyber Security 706
Response: Thank you for your comments. Please refer to the response to comments document.				
David L Kiguel	Hydro One Networks, Inc.	3	Negative	Hydro One is casting a negative vote for the following reasons: 1. We do not believe the standard will result in an improvement in reliability since the revisions merely replace the risk-based assessment methodology with a list of criteria that will ultimately result in inclusion of facilities on the Critical Assets list that are non-impactive on the BES. 2. We do not agree with criteria 1.6 and 1.7 in Attachment 1 as written. Application of these criteria would result in the inclusion of facilities that will have no impact on the BES reliability. We believe that the list of applicable facilities should be determined following an impact-based assessment to be performed by the Reliability Coordinator. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct/review the assessment should be included. We therefore propose the following wording to replace 1.6 and 1.7 in Attachment 1: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will have no

Voter	Entity	Segment	Vote	Comment
				impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission Facilities operated at 300 kV or higher to less than 500 kV at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages. 3. We do not agree with the removal of the exclusion that applies to facilities regulated by the Canadian Nuclear Safety Commission from the Applicability Section, This explicit statement makes it clear that CIP standards do not apply to those facilities which would not be the case if it were removed.
Response: Thank you for your comments. 1) The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology. 2) Items 1.6 and 1.7 – The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. 3) The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
Theodore J Hilmes	KAMO Electric Cooperative	3	Negative	please review submitted comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Gregory David Woessner	Kissimmee Utility Authority	3	Negative	KUA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA. That needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives on KUA's views.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Stephen D Pogue	M & A Electric Power Cooperative	3	Negative	Please review submitted comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Darl Shimko	Madison Gas and Electric Co.	3	Negative	The comments, below, are issues that the SDT should address before the next ballot. Q1 through Q6 refer to questions in the Unofficial Comment Form for Project 2008-06. Q1: We do not believe the proposed standard will lead to an improvement in reliability in all cases. If a bright line is used, it removes all engineering analysis the entity is currently performing with the current CIP-002-3 methodology. This may bring in or remove assets for this Standard. A bright-line approach may be useful to a smaller entity, but may not be in the best interest to larger entities. The SDT should consider a bright line with a MW threshold for physical unit size or MW loads for control centers, see comments below. Q2: Suggested improvements to Attachment 1: Criterion Number 1.5 -- Based on the Rationale Document, please clarify that Facilities within the Cranking Paths will be assigned the Critical Asset identification up to the point where multiple path options exist. Criterion Number 1.13 -- Based on the Rationale Document, please clarify that the 300 MW level applies to a single common control system and not multiple like systems such as those installed for UFLS protection (multiple identical or similar individual, but independent, relays that may shed 300 MW's or more in aggregate, but individually shed less than 300 MW). Criterion Number 1.14 -- Based on the Rationale Document, every RC, BA, and TOP's control center, control system, backup control center and backup control system is Critical due to EOP-008. EOP-008-0 is the FERC approved Standard for US entities. We note the purpose of EOP-008-0 is: "Each reliability entity must have a plan to continue reliability operations in the event its control center becomes inoperable". Furthermore, the SDT quoted EOP-008-1 in the Rational Document, which is not FERC approved. The SDT needs to consider this when writing a continental wide Standard. The phrase in the Rationale Document, "While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets", is unjustified. Assuming a BA controls no critical assets qualified as such by other criteria, a BA that, in aggregate, controls relatively small amounts of

Voter	Entity	Segment	Vote	Comment
				real and/or reactive power clearly has less of an effect on reliability than a BA that controls relatively large amounts of such resources. Indeed, the fact that "size matters" is recognized by Criteria 1.1, 1.2, 1.6, 1.7, 1.13, and 1.15. Criterion 1.14 should be modified to recognize this conclusion by including relevant quantitative thresholds. Thresholds that were proposed in CIP-010 Criteria 1.13 and 1.14 would be reasonable. In any event, the thresholds for the BA control center or control system should be no more inclusive than those used to qualify the individual assets controlled by the BA. To complicate matters, presently there are 28 Local Balancing Authorities (LBA's) that are part of the Midwest ISO BA Area (JRO00001). These entities do not perform all the BA functional obligations as stated in the Rationale Document (the MISO BA performs the majority of BAL-001 through BAL-005). Furthermore, the scopes of operation of the LBA's span a wide range from small to large and few too many resources. This underscores the need to not assume that any BA (or LBA) that performs or supports any BA function or part of a BA function is necessarily critical to BES reliability. Please provide the analysis and justification to how these entities fit into the BA requirement as stated in 1.14. If it is the intent of the SDT to capture the generation within the balancing functions of a BA, the SDT has that covered by Criteria 1.15. Q3: While we agree with the general requirement of R1, we do not agree with certain aspects of Attachment 1 - Critical Asset Criteria, as discussed in previous comments, above. Q4: We agree with R2. Q5: The implementation plan is clear and reasonable regarding entities that either in the past have identified they have CA's, or have never identified CA's. However, there is an issue when an entity has previously identified one type of asset as critical and then later identifies another type of critical asset. For example, a control center was previously identified as being a CA. Later, the entity identifies a cranking path or Blackstart generator as being a CA. It is recommended that if an asset dissimilar to previously identified critical assets is identified as a CA, that the entity is given 24 months to become compliant. This time is needed since the entity is now in an area that they may have not dealt with in the past. Q6: The implementation plan for newly identified CCAs should allow 24 months to become compliant when the newly identified CCAs are associated with newly identified critical assets of a type that was not previously identified as critical. See Comment Q5, above.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Q1: The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology throughout North America. Q2: Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." It is appropriate to refer to an industry-approved and NERC BOT-approved standard in a guidance document, even if it has not been accepted at FERC. Q3: Please refer to response to Q2 above. Q4: Thank you. Q5: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset. Q6: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Greg C. Parent	Manitoba Hydro	3	Negative	Please see comments submitted by Manitoba Hydro in the formal comment period.
Response:Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Don Horsley	Mississippi Power	3	Negative	Comments were submitted via Comment Form: Project 2008-06 - Cyber Security 706
Response: Thank you for your comments. Please refer to the response to comments document.				
Steven M. Jackson	Municipal Electric Authority of Georgia	3	Negative	MEAG supports the APPA's comments submitted to the NERC CIP standard drafting team.
Response: Thank you for your comments. Please refer to the response to comments document.				
John S Bos	Muscatine Power & Water	3	Negative	Just because a Balancing Authority or Transmission Operator has a control center or back-up control center should not automatically cast those control centers as Critical Assets. A BA or TOP with a small system (very small native system load, generation, and very minor transmission system) should not be forced into the CIP compliance world just because they have control centers. This is an incredible expense for a small utility. If control centers are to be determining factors for inclusion of a small BA or TOP under CIP-002 V4, there should be criteria developed based on the size of the utility. For instance, a BA or TOP with control centers serving a native system of greater than X MW would be considered for inclusion. Or a BA or TOP with control centers and a transmission system of greater than X miles would be considered for inclusion. Or a BA or TOP with control centers and greater than X MW of generation on their system would be considered for inclusion. Forcing small vertically-integrated utilities with exceedingly minor impact on the BES into the CIP compliance world is not equitable.
Response: Thank you for your comments. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				

Voter	Entity	Segment	Vote	Comment
Tony Eddleman	Nebraska Public Power District	3	Negative	NPPD comments are addressed by comments submitted through the American Public Power Association (APPA). We agree with and support the APPA comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	Negative	Please review submitted comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Rick Keetch	NRG Energy Power Marketing, Inc.	3	Negative	Pertaining to CIP-002-4 R1, the following need to be addressed in Attachment 1: 1.1 - Add capacity factor as a qualifier for exclusion below an established low threshold. 1.3 - Mandate coordination/approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. These classifications and approvals need to take into consideration 5 year forecasts for planning and budgeting purposes.. 1.5 - TOP needs to define the cranking path in restoration plan to the affected entities to adequately secure these restoration paths.. 1.9 - Please explain FACTS - need definition 1.10 - Need coordination between TOP & GO to identify critical assets. 1.15 - How is the 1500 MW aggregate determined? Is it an aggregate of generator name plates or the sum of controllable megawatts between a unit's high and low limits? General: Attachment 1 needs to have defined terms for capability, plant, control center Requirement 2 needs to clarify the following items: 1) Need Clarification on routable path, discrete links and serial connections as it pertains to CIP-002-3 R3: Is a device considered to communicate outside the ESP using routable protocol if ANY portion of the communications path uses routable protocol? 2)Need clarification concerning shared assets. Does it mean shared between a single device or same device on a network? 3)R2 states that only shared cyber assets for a group of generating units at

Voter	Entity	Segment	Vote	Comment
				a single location identified in Attachment 1 criteria 1.1, namely the 1500 MWs brightline, that could impact reliable operation, should be considered. Does this cyber asset identification only include assets meeting criteria 1.1 and therefore exclude any cyber assets utilized for reliable operation of a designated critical asset such as a single blackstart resource? Please provide clarification in this requirement.

Response: Thank you for your comments.

Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.

Item 1.3 –This criterion has been reworded to, "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Item 1.9 – FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability."

Item 1.10 – The assets would be identified by the asset owners. It is agreed that communication between GOs and TO/TOPs will be required.

Item 1.15 – This is the aggregate highest rated net Real Power capability output of all generation under dispatch/control.

At this time, the SDT is choosing not to add "capability," "plant," or "control center" to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.

The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1.

David McDowell	NW Electric Power Cooperative, Inc.	3	Negative	Please review submitted comments.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Ballard Keith Mutters	Orlando Utilities Commission	3	Negative	See comments submitted on behalf or Orlando Utilities Commission.
Response: Thank you for your comments. Please refer to the response to comments document.				
Richard H. Chapman	Owensboro Municipal Utilities	3	Negative	There is too much ambiguity in Attachment 1 1.14, the Critical Control Center definition needs further clarification controlling either a specified load or specified voltage level.
Response: Thank you for your comment. Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, also has been added which states, " Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Michael Mertz	PNM Resources	3	Negative	PNM Resources applauds the significant effort of the SDT in developing the revision to CIP-002-4, and conforming changes to CIP-003-4 through CIP-009-4. Although the most recent version of CIP-002-4 represents significant progress, PNM Resources must cast a negative vote with the following comments: The criteria related to blackstart resources do not consider the varying role of blackstart resources identified in restoration plans, and as drafted, will require identification of any blackstart resource, or path, mentioned in a restoration plan to be identified as a Critical Asset. Entities in many regions may identify a significant number of Blackstart Resources in a restoration plan, representing primary and alternate resources allowing for a number of options for system restoration. PNM Resources recommends the following revisions to the criteria: 1.4. Each primary Blackstart Resource essential to the Transmission Operator's restoration plan. 1.5. The Facilities comprising the primary Cranking Paths and initial switching requirements from the primary Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on

Voter	Entity	Segment	Vote	Comment
				the Cranking Path where multiple path options exist.
Response: Thank you for your comments. Items 1.4 and 1.5 – The SDT considered using the word "primary," but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.				
Jeffrey Mueller	Public Service Electric and Gas Co.	3	Negative	Please see PSEG Companies' comments filed separately. The PSEG companies will change the vote to affirmative if the comments are adequately addressed by the drafting team.
Response: Thank you for your comments. Please refer to the response to comments document.				
James Leigh-Kendall	Sacramento Municipal Utility District	3	Negative	After reviewing the proposed version 4 language for CIP-002, R2, the placement of the additional text on generation is confusing. It appears to be trying to accomplish two different purposes. SMUD does not have any objections to the text itself, just the placement. SMUD proposes organizing the requirement as follows: R2. Critical Cyber Asset Identification- Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall review this list at least annually, and update it as necessary. R2.1 For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.1.2 The Cyber Asset uses a routable protocol within a control center; or, R2.1.3 The Cyber Asset is dial-up accessible. R2.2 For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1., the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Additionally, SMUD, as a member of APPA, would like to reflect its support

Voter	Entity	Segment	Vote	Comment
				to those CIP-002-4 Standard comments submitted by APPA staff.
Response: Thank you for your comments. Please refer to the response to comments document for responses to APPA comments. Requirement R2 has been changed to clarify the issues presented.				
John T. Underhill	Salt River Project	3	Negative	SRP believes that a bright line assessment methodology for determining Critical Assets is not in the best interest of reliability. This is especially true in the designation of substations and generating facilities. The attributes of these stations and their unique impact on Bulk Electric System reliability must be taken into account. There are several terms and phrases used within Requirement 2 of the proposed Standard that need to be better defined to eliminate ambiguity. These terms are: 1) essential to the operation of the Critical Asset, 2) adversely impact the reliable operation needs to be defined; and, 3) within 15 minutes. We believe the CIP-002-4 implementation plan for newly identified Critical Assets and associated Critical Cyber Assets provides inadequate time. SRP suggests the implementation timeframe be extended to 30 months after the effective date of the Standard.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about (annual) exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version Thank you for your comment. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Scott Peterson	San Diego Gas & Electric	3	Negative	SDG&E has submitted suggested changes that it feels should be incorporated before it can vote in favor of the revision.
Response: Thank you for your comments. Please refer to the response to comments document.				
Jeff L Neas	Sho-Me Power Electric	3	Negative	Please review submitted comments.

Voter	Entity	Segment	Vote	Comment
	Cooperative			
Response: Thank you for your comments. Please refer to the response to comments document.				
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace? 1 Yes 0 No Comments: We understand that the errata, which removes discussion of the "risk-based assessment methodology" from the proposed CIP-002-4 standard, would also apply to the mapping document. We appreciate the bright-line clarification to ensure consistent identification of Critical Assets throughout the industry. 2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: We suggest that the functional entities Planning Coordinator and Transmission planner be added to the applicability section. Feedback on specific criteria as follows: 1.1, We request clarification on the phrase "single plant location". This phrase is not defined and it is not clear what level of proximity of generators would be considered a "single plant location". Rather than discuss this in terms of geography (location), we feel it would be better to discuss in terms of "Each group of generating units (including nuclear generation), operated using common cyber control systems other than the Control Centers identified in 1.14 and 1.15, with an aggregate...". 1.3, We suggest the wording: "Each generation facility designated by the Planning Coordinator or Transmission Planner as required to avoid one or more reliability criteria violations". 1.4, The blackstart units deemed critical should be only those identified by the Transmission Operator to meet the minimum critical blackstart requirement. The resulting suggested wording would be: "Each Blackstart Resource identified in the Transmission Operator's restoration plan required to meet the minimum critical blackstart requirement". 1.8, We suggest the wording: "Transmission Facilities at a single location that the Planning Coordinator or Transmission planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL)

Voter	Entity	Segment	Vote	Comment
				violations". 1.9, We suggest similar wording: "…unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations". 1.11, We suggest the following wording: "Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements". 1.12, We suggest the following wording: "…unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed". 1.14, We suggest this be made consistent with 1.15, i.e. "Each control center, or backup control center, used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator". 1.16, We suggest the following wording: "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include". 3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification - Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: 4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: Although we agree with the

Voter	Entity	Segment	Vote	Comment
				proposed Requirement R2, We are concerned that the document "CIP-002-4 Cyber Security - Critical Cyber Asset Identification: Rationale and Implementation Reference Document" actually appears to provide more rationale and guidance on Critical Assets than Critical Cyber Assets. 5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: 6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement. 0 Yes 1 No Comments: We believe that it would be better to simply have a uniform 18 month implementation deadline for newly identified CCAs rather than have different timelines for different requirements. This will simplify reporting and streamline efforts to become fully compliant. We understand that nuclear timelines are subject to NRC requirements and the necessity of accomplishing some tasks only during refueling outages appropriately dictates a separate schedule for them.

Response: Thank you for your comments.

Q2. Since there is no Requirement that applies to the Planning Coordinator or the Transmission Planner, it is not appropriate to include them in the Applicability section.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.

Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or

Voter	Entity	Segment	Vote	Comment
Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. Q4. Thank you for your comments. The SDT will reexamine the guidance document. Q5. Due to the limited scope of version 4, the SDT is only making conforming changes to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.				
Allen Mosher	American Public Power Association	4	Negative	See group comments submitted by the APPA CIP Task Force.
Response: Thank you for your comments. Please refer to the response to comments document.				
Shamus J Gamache	Central Lincoln PUD	4	Negative	Please see comments posted by Steve Alexanderson at Central Lincoln.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
David Frank Ronk	Consumers Energy	4	Negative	In Criteria 1.4, we would prefer to see Blackstart Resources for primary paths only specified. The way it is written, all Blackstart Resources, including those for alternate paths, would be included. This creates ambiguity as there are very many possible alternate cranking paths. We dislike Criteria 1.5 and the wording in the Rationale Document. Similar to 1.4, the words "primary path" are no longer used and depending on interpretation, additional resources on what are now alternate cranking paths could be brought into play. The Standard should be clear and not subject to interpretation.
Response: Thank you for your comments. Items 1.4 and 1.5 – The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.				
Rick Syring	Cowlitz County PUD	4	Negative	The Attachment will wrongfully include some assets as critical. Please refer to Cowlitz County PUD comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Frank Gaffney	Florida Municipal Power Agency	4	Negative	FMPA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Thomas W. Richards	Fort Pierce Utilities Authority	4	Negative	FPUA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified. Please see FMPA's group comments submitted on our behalf through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				
Bob C. Thomas	Illinois Municipal Electric Agency	4	Negative	IMEA appreciates the SDT's efforts to simplify CIP-002. IMEA believes it will be in a position to affirm this proposed Reliability Standard revision after comments on Draft 1 and comments during balloting are addressed. IMEA supports comments submitted by the American Public Power Association. In addition, as IMEA commented, we recommend Criterion 1.8 be continued with the following language: "...(IROLs) as demonstrated by the Reliability Coordinator." If the RC is not appropriate, it will be necessary to add the appropriate functional entity, for demonstrating IROLs, to Applicability Secion 1.4. This addional language will clarify that the TO, LSE, etc. is not responsible for demonstrating IROLs.
Response: Thank you for your comments. Please refer to the response to comments document for responses to APPA's comments. Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."				
Christopher Plante	Integrys Energy Group, Inc.	4	Negative	We believe that a bright line criteria as proposed by the ballot will improve the reliability and safety of the BES. However, changes as provided by MRO's NSRS need to be incorporated into the proposed standard to eliminate the potential for arbitrary application and capricious enforcement of the standard.
Response: Thank you for your comments. Please refer to the response to comments document.				
Richard Comeaux	LaGen	4	Negative	Pertaining to CIP-002-4 R1, the following need to be addressed in Attachment 1:

Voter	Entity	Segment	Vote	Comment
				1.1 - Add capacity factor as a qualifier for exclusion below an established low threshold. 1.3 - Mandate coordination/approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. These classifications and approvals need to take into consideration 5 year forecasts for planning and budgeting purposes.. 1.5 - TOP needs to define the cranking path in restoration plan to the affected entities to adequately secure these restoration paths.. 1.9 - Please explain FACTS - need definition 1.10 - Need coordination between TOP & GO to identify critical assets. 1.15 - How is the 1500 MW aggregate determined? Is it an aggregate of generator name plates or the sum of controllable megawatts between a unit's high and low limits? General: Attachment 1 needs to have defined terms for capability, plant, control center Requirement 2 needs to clarify the following items: 1) Need Clarification on routable path, discrete links and serial connections as it pertains to CIP-002-3 R3: Is a device considered to communicate outside the ESP using routable protocol if ANY portion of the communications path uses routable protocol? 2)Need clarification concerning shared assets. Does it mean shared between a single device or same device on a network? 3)R2 states that only shared cyber assets for a group of generating units at a single location identified in Attachment 1 criteria 1.1, namely the 1500 MWs brightline, that could impact reliable operation, should be considered. Does this cyber asset identification only include assets meeting criteria 1.1 and therefore exclude any cyber assets utilized for reliable operation of a designated critical asset such as a single blackstart resource? Please provide clarification in this requirement.

Response: Thank you for your comments.

Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Voter	Entity	Segment	Vote	Comment
Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan." Item 1.9 – FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability." Item 1.10 – The assets would be identified by the asset owners. It is agreed that communication between GOs and TO/TOPs will be required. Item 1.15 – This is the aggregate highest rated net Real Power capability output of all generation under dispatch/control. At this time, the SDT is choosing not to add "capability," "plant," or "control center" to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect. The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1.				
Joseph G. DePoorter	Madison Gas and Electric Co.	4	Negative	The below are outstanding issues that the SDT should address before the next ballot. Comments are in line with the Unofficial Comment Form for Project 2008-06. Q1: No, If a brightline is used, it removes all engineering analysis the entity is currently performing with the current CIP-002-3 methodology. This may bring in or remove assets for this Standard. A brightline approach may be useful to a smaller entity but may not be in the best interest to larger entities. The SDT should consider a brightline with a MW threshold for physical unit size or MW loads for control centers, see comments below. Q2: Yes, Criteria number 1.5; Based on the Rationale Document, please clarify that Facilities within the Cranking Paths will be assigned the Critical Asset identification up to the point where multiple path options exist. Criteria number 1.13; Based on the Rationale Document, please clarify that the 300 MW level applies to a single common control system and not multiple like systems such as those installed for UFLS protection (multiple identical or similar individual, but independent, relays that may shed 300 MW's or more in aggregate, but individually shed less than 300 MW). Criteria number 1.14; Based on the Rationale Document, every RC, BA, and TOP's control center, control system, backup control center and backup control system is Critical due to EOP-008. EOP-008-0 is the FERC approved

Voter	Entity	Segment	Vote	Comment
				Standard for US entities. The purpose of EOP-008-0 is: “Each reliability entity must have a plan to continue reliability operations in the event its control center becomes inoperable”. The SDT quoted EOP-008-1 in the Rational Document, which is not FERC approved. The SDT needs to consider this when writing a continental wide Standard. The phrase in the Rationale Document: “While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets”, is unjustified. Assuming a BA controls no critical assets qualified as such by other criteria, a BA that, in aggregate, controls relatively small amounts of real and/or reactive power clearly has less of an effect on reliability than a BA that controls relatively large amounts of such resources. Indeed, the fact that "size matters" is recognized by Criteria 1.1, 1.2, 1.6, 1.7, 1.13, and 1.15. Criterion 1.14 should be modified to recognize this conclusion by including relevant quantitative thresholds. Thresholds that were proposed in CIP-010 Criteria 1.13 and 1.14 would be reasonable. In any event, the thresholds for the BA control center or control system should be no more inclusive than those used to qualify the individual assets controlled by the BA. To complicate matters, presently there are 28 Local Balancing Authorities (LBA’s) that are part of the Midwest ISO BA Area (JRO00001). These entities do not perform all the BA functional obligations as stated in the Rationale Document (the MISO BA performs the majority of BAL-001 through BAL-005). Furthermore, the scopes of operation of the LBA’s span a wide range from small to large and few too many resources. This underscores the need to not assume that any BA (or LBA) that performs or supports any BA function or part of a BA function is necessarily critical to BES reliability. Please provide the analysis and justification to how these entities fit into the BA requirement as stated in 1.14. If it is the intent of the SDT to capture the generation within the balancing functions of a BA, the SDT has that covered by Criteria 1.15. Q3: Disagree, While we agree with the general requirement of R1, we do not agree with certain aspects of Attachment 1 - Critical Asset Criteria, as discussed in responses to previous questions, above. Q4: Agree Q5: No, The implementation plan is clear on entities that either have in the past, identified they have CA’s or have not ever identified CA’s. The issue is present that what happens when an entity has only identified a control center as being a CA. But now they have identified a cranking path or Blackstart generator as being a CA. It is recommended that if non like items are identified as a CA, that the entity is given 24 months to become

Voter	Entity	Segment	Vote	Comment
				compliant. This will allow the entity enough time since they are now in an area that they may have not dealt with in the past. Q6: No, See question 5.

Response: Thank you for your comments.

Q1: The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology throughout North America.

Q2: Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize.

Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." It is appropriate to refer to an industry approved and NERC BOT approved standard in a guidance document, even if it has not been accepted at FERC.

Q3: Please refer to response to Q2 above.

Q4: Thank you.

Q5: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Q6: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Voter	Entity	Segment	Vote	Comment
Mark Ringhausen	Old Dominion Electric Coop.	4	Negative	All of the following comments apply to the Attachment 1: General Comments: For the cases where any other entity (PC/TP) would declare that other entity has a Critical Asset, there must be a phase-in compliance process to allow the entity with the CA to get into compliance with the CIP requiorments. Also, there must be a due process procedure to allow the entity with the designated CA to challenge this at the Region or NERC level. 1.3: PC/TP must have a formal process to determine whether or not a generation faciltiy is needed for reliabiltiy or not. This process must be provided to each generation owner and operator under review by the PC/TPs. 1.5: The Cranking Paths adn initial switching requirements must be provided by the TOP to the TO in cases where these are two different entities. 1.10: You need to better described which facilities you are trying to cover here. Any transmission facility which if lost would result in the loss of >1500MWs or a PC/TP designated generation facility for reliability. 1.13: Should match 1.1, change 300MWs to 1500MWs. Impact of losing 1500MWs of generation is still greater than losing 1500MWs of load.

Response: Thank you for your comments.

The burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. The Responsible Entity has to check with its Planning Coordinator or Transmission Planner on whether its unit is designated, or what other units are designated as required for reliability reasons. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, then that unit must be classified as a Critical Asset. If an entity feels that they have an asset that has been unjustly classified as required for reliability reasons, there are appeals processes that can be used.

Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any transmission Facility that, if lost, would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include the partial or total loss of a substation. This criterion has been changed to "Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1

Voter	Entity	Segment	Vote	Comment
or 1.3." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."				
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	The way CIP-002-4 attachment 1 - 1.13 is worded is a concern- would any RE with a load over 970 MW in the Western Interconnection have critical assets just because their UFLS scheme has armed 31% of their load-meeting the 300 MW threshold? There are already PRC standards to address these systems, so we don't believe that the 300 MW "bright line" threshold is reasonable.
Response: Thank you for your comments. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."				
Mike Ramirez	Sacramento Municipal Utility District	4	Negative	After reviewing the proposed version 4 language for CIP-002, R2, the placement of the additional text on generation is confusing. It appears to be trying to accomplish two different purposes. SMUD does not have any objections to the text itself, just the placement. SMUD proposes organizing the requirement as follows: R2. Critical Cyber Asset Identification- Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall review this list at least annually, and update it as necessary. R2.1 For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.1.2 The Cyber Asset uses a routable protocol within a control center; or, R2.1.3 The Cyber Asset is dial-up accessible. R2.2 For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1., the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Additionally, SMUD, as a member of APPA, would like to reflect its support to those CIP-002-4 Standard comments submitted by APPA staff.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document for responses to APPA comments. Requirement R2 has been changed to clarify the issues presented.				
Anthony Jankowski	Wisconsin Energy Corp.	4	Negative	Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply. 1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace? 1 Yes 0 No Comments: We understand that the errata, which removes discussion of the "risk-based assessment methodology" from the proposed CIP-002-4 standard, would also apply to the mapping document. We appreciate the bright-line clarification to ensure consistent identification of Critical Assets throughout the industry. 2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: We suggest that the functional entities Planning Coordinator and Transmission planner be added to the applicability section. Feedback on specific criteria as follows: 1.1, We request clarification on the phrase "single plant location". This phrase is not defined and it is not clear what level of proximity of generators would be considered a "single plant location". Rather than discuss this in terms of geography (location), we feel it would be better to discuss in terms of "Each group of generating units (including nuclear generation), operated using common cyber control systems other than the Control Centers identified in 1.14 and 1.15, with an aggregate...". 1.3, We suggest the wording: "Each generation facility designated by the Planning Coordinator or Transmission Planner as required to avoid one or more reliability criteria violations". 1.4, The blackstart units deemed critical should be only those identified by

Voter	Entity	Segment	Vote	Comment
				the Transmission Operator to meet the minimum critical blackstart requirement. The resulting suggested wording would be: "Each Blackstart Resource identified in the Transmission Operator's restoration plan required to meet the minimum critical blackstart requirement". 1.8, We suggest the wording: "Transmission Facilities at a single location that the Planning Coordinator or Transmission planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations". 1.9, We suggest similar wording: "...unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations". 1.11, We suggest the following wording: "Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements". 1.12, We suggest the following wording: "...unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed". 1.14, We suggest this be made consistent with 1.15, i.e. "Each control center, or backup control center, used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator". 1.16, We suggest the following wording: "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include". 3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification - Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: 4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed

Voter	Entity	Segment	Vote	Comment
				Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: Although we agree with the proposed Requirement R2, We are concerned that the document "CIP-002-4 Cyber Security - Critical Cyber Asset Identification: Rationale and Implementation Reference Document" actually appears to provide more rationale and guidance on Critical Assets than Critical Cyber Assets. 5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: 6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement. 0 Yes 1 No Comments: We believe that it would be better to simply have a uniform 18 month implementation deadline for newly identified CCAs rather than have different timelines for different requirements. This will simplify reporting and streamline efforts to become fully compliant. We understand that nuclear timelines are subject to NRC requirements and the necessity of accomplishing some tasks only during refueling outages appropriately dictates a separate schedule for them.

Response: Thank you for your comments.

Q2. Since there is no Requirement that applies to the Planning Coordinator or the Transmission Planner, it is not appropriate to include them in the Applicability section.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Voter	Entity	Segment	Vote	Comment
				Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. The present wording is appropriate. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. Q4. Thank you for your comments. The SDT will reexamine the guidance document. Q5. Due to the limited scope of version 4, the SDT is only making conforming changes to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

Voter	Entity	Segment	Vote	Comment
Brock Ondayko	AEP Service Corp.	5	Negative	Overall, AEP is supportive of the efforts and the general concepts of this draft; however, there are a few refinements that will enhance the requirements and remove ambiguity. AEP encourages the SDT to consider the items below in a future draft of the standard: AEP would contend that there are regional differences that would be relevant to determine a MW threshold for generators. We support the concept that was contained in the last draft that made the determination based on the capacity reserves. However, the prior language would need to be revisited to ensure that value was fixed for a period of time. In addition, requirement 2.2 uses the term control center (also used in attachment 1) that is not a NERC defined term. This will introduce ambiguity to implementation. There has been ongoing confusion regarding the difference between "control centers" and "control rooms." We do not believe that a "control room" at a power plant or a substation would be considered a "control center." There is language in the NERC Security Guideline for Electricity Sector: Identifying Critical Assets document that the SDT should consider and incorporate into the NERC Glossary. Net real power capability testing is defined in MOD-024 standards that have yet to be FERC approved. Furthermore, not all of the regions have defined the parameters for the capability testing.
Response: Thank you for your comments. Item 1.1 - In prior versions we had wording about reserve sharing for the threshold. We received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. We did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. At this time, the SDT is choosing not to add control center to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. CIP-002-4 does not require net real power capability testing.				
Brad Haralson	Associated Electric Cooperative, Inc.	5	Negative	please see submitted comments

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Clement Ma	BC Hydro and Power Authority	5	Negative	Critical Assets List comments 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations The present wording uses an arbitrary numbers of stations, the number of stations is immaterial BCH recommends the "Transmission Facilities operated at 300 kV or higher that if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs). 1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. A clear definition of common control system(s) is required. Is under frequency or under voltage load shedding schemes considered control systems? The load shedding of 300 MW or more does it include firm or interruptible load or both? 1.16. Any additional assets that the Responsible Entity deems appropriate to include. To encourage reliability the additional assets deemed appropriate by a Responsible Entity should not be auditable.
Response: Thank you for your comments. Item 1.7 – In order to be more accurate in terms of the impact, the drafting team thought that it was more appropriate to refer to the number of connected transmission substations instead of using IROLs. The intent was to avoid double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them. This includes upstream, downstream, radial and networked substations. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.				
Francis J. Halpin	Bonneville Power Administration	5	Negative	Please refer to BPA comments submitted during the formal comment period on 10/26/10
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Jeff Mead	City of Grand Island	5	Negative	I echo the MRO NSRS comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
Alan Gale	City of Tallahassee	5	Negative	The City of Tallahassee supports APPA's comments.
Response: Thank you for your comments. Please refer to the response to comments document.				
James B Lewis	Consumers Energy	5	Negative	In Criteria 1.4, we would prefer to see Blackstart Resources for primary paths only specified. The way it is written, all Blackstart Resources, inlcuding those for alternate paths, would be included. This creates ambiguity as there are very many possible alternate cranking paths. We dislike Criteria 1.5 and the wording in the Rationale Document. Similar to 1.4, the words "primary path" are no longer used and depending on interpretation, additional resources on what are now alternate cranking paths could be brought into play. The Standard should be clear and not subject to interpretation.
Response: Thank you for your comments. Items 1.4 and 1.5 – The SDT considered using the word “primary”, but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. A Blackstart Resource is defined as “A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator’s restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator’s restoration plan.” EOP-005-2 R1.4 states that the restoration plan must include “Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.” The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.				
Bob Essex	Cowlitz County PUD	5	Negative	The Attachment is too inclusive. Please refer to Cowlitz County PUD and APPA comments.
Response: Thank you for your comments. Please refer to the response to comments document.				

Voter	Entity	Segment	Vote	Comment
Robert B Stevens	CPS Energy	5	Negative	I believe the standard is going the correct direction. However, I would modify one definition on the Attachment. The Attachment reads "generating units (including nuclear generation) at a single plant location" I would propose the same language but add "connected to transmission grid at one location or one buss", or something similar. The problem arises where you have multiple generating units at one plant location, but a set of plants feed into 345 switchgear and a set of plants feeds into 138 switchgear. You have two distinct reliability situations, thus the need to distinguish.
Response: Thank you for your comments. Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.				
Mike Garton	Dominion Resources, Inc.	5	Negative	Dominion conceptually supports bright line criteria for determining critical assets. However, we cannot vote in favor at this time because we believe that changes are needed in Table 2 that recognize the implementation for infrastructure (physical and electronic security) should be equal to, or longer than, that required for training. We also believe that the bright line criteria for generation control center needs further effort. Please see more specific comments/recommendation submitted by Dominion.
Response: Thank you for your comments. Please refer to the response to comments document.				
Stephen Ricker	East Kentucky Power Coop.	5	Negative	EKPC would suggest rewording R2 to say: "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those interconnected Cyber Assets that collectively could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes."
Response: Thank you for your comments. Requirement R2 has been changed based on industry comments received.				
Stanley M Jaskot	Entergy Corporation	5	Negative	Switchyards serving nuclear facilities should not be automatically classified as critical assets. The fact that a BES switchyard serves a nuclear facility should not in itself qualify the switchyard as a critical asset. While nuclear units and their support facilities may qualify as critical assets under a

Voter	Entity	Segment	Vote	Comment
				separate set of criteria, they should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability. All blackstart units and associated cranking paths should not be automatically classified as critical assets. Blackstart units may be useful in the restoration of the BES following a large scale outage, but they are not necessarily essential to the reliability of the BES under normal operation. Blackstart units should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability. In addition, just using a MW or MVAR rating alone in determining critical assets is not enough. It needs to be coupled with a service factor because we have a large generating station thay runs very infrequently and should not be deemed critical based on its operation. In addition, Entergy presented many other comments and suggested changes during the development of this draft standard. Entergy continues to support those comments even though some were not incorporated into this standard.
Response: Thank you for your comments. Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources. Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.				
David Schumann	Florida Municipal Power Agency	5	Negative	FMPA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that

Voter	Entity	Segment	Vote	Comment
				needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				
Brent Hebert	Horizon Wind Energy	5	Negative	Part 1.15 designates generation control centers that control generation Facilities used to control generation greater than an aggregate of 1500 MW in a single interconnection and was based on the bright-line used in Part 1.1. Part 1.1 includes generation at a single plant location (with-in a single BA or RSG). Part 1.15 should be more in line with part 1.1 where the generation control center controlling generation with an aggregate of 1500 MW or more within a single BA or RSG be designated as critical. It is true that the span of control of a generation control center may cross multiple BAs or RSG, but the control of generation within a single BA or RSG could fall well below the 1500 MWs in Part 1.1. even if located in a single interconnection.
Response: Thank you for your comments. Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection."				
Dennis Florom	Lincoln Electric System	5	Negative	Please review the comments submitted by the MRO's NERC Standards Review Subcommittee for LES' reasons for a negative ballot.
Response: Thank you for your comments. Please refer to the response to comments document.				
Mike Laney	Luminant Generation Company LLC	5	Negative	Luminant Generation Company LLC (Luminant Generation) thanks the Standard Drafting Team (SDT) for their work on the NERC CIP Cyber Security Standards and for the opportunity to provide input into the standards development process. Although Luminant Generation has voted "Negative" on the current draft standard, Luminant Generation supports the SDT goal of completing the revision of CIP-002-4 by December 2010, and believes with some modification to the Attachment 1 Criteria, the goal is still achievable. Specifically, Luminant Generation is concerned that Criteria 1.3 has no defined basis for determining the reliability need of a generation Facility. As written, the Planning Coordinator or Transmission Planner could use any

Voter	Entity	Segment	Vote	Comment
				basis, or conversely, no basis, for designating a generation Facility as required for reliability purposes. For Criteria 1.8, 1.9, and 1.12, the SDT has appropriately used the violation of an Interconnection Reliability Operating Limit (IROL) as the basis for determining the reliability need of transmission Facilities. Luminant Generation believes this same basis is appropriate for application to generation Facilities in Criteria 1.3, and offers the following language for consideration by the SDT: 1.3 "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes, by demonstrating that the generation facility, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs)."
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."				
Steven Schultz	Madison Gas and Electric Co.	5	Negative	The below are outstanding issues that the SDT should address before the next ballot. Comments are in line with the Unofficial Comment Form for Project 2008-06. Q1: No, If a brightline is used, it removes all engineering analysis the entity is currently performing with the current CIP-002-3 methodology. This may bring in or remove assets for this Standard. A brightline approach may be useful to a smaller entity but may not be in the best interest to larger entities. The SDT should consider a brightline with a MW threshold for physical unit size or MW loads for control centers, see comments below. Q2: Yes, Criteria number 1.5; Based on the Rationale Document, please clarify that Facilities within the Cranking Paths will be assigned the Critical Asset identification up to the point where multiple path options exist. Criteria number 1.13; Based on the Rationale Document, please clarify that the 300 MW level applies to a single common control system and not multiple like systems such as those installed for UFLS protection (multiple identical or similar individual, but independent, relays that may shed 300 MW's or more in aggregate, but individually shed less than 300 MW). Criteria number 1.14; Based on the Rationale Document, every RC, BA, and TOP's control center, control system, backup control center and backup control system is Critical due to EOP-008. EOP-008-0 is the FERC approved Standard for US entities. The purpose of EOP-008-0 is: "Each reliability entity must have a plan to continue reliability operations in the event its

Voter	Entity	Segment	Vote	Comment
				control center becomes inoperable". The SDT quoted EOP-008-1 in the Rational Document, which is not FERC approved. The SDT needs to consider this when writing a continental wide Standard. The phrase in the Rationale Document: "While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets", is unjustified. Assuming a BA controls no critical assets qualified as such by other criteria, a BA that, in aggregate, controls relatively small amounts of real and/or reactive power clearly has less of an effect on reliability than a BA that controls relatively large amounts of such resources. Indeed, the fact that "size matters" is recognized by Criteria 1.1, 1.2, 1.6, 1.7, 1.13, and 1.15. Criterion 1.14 should be modified to recognize this conclusion by including relevant quantitative thresholds. Thresholds that were proposed in CIP-010 Criteria 1.13 and 1.14 would be reasonable. In any event, the thresholds for the BA control center or control system should be no more inclusive than those used to qualify the individual assets controlled by the BA. To complicate matters, presently there are 28 Local Balancing Authorities (LBA's) that are part of the Midwest ISO BA Area (JRO00001). These entities do not perform all the BA functional obligations as stated in the Rationale Document (the MISO BA performs the majority of BAL-001 through BAL-005). Furthermore, the scopes of operation of the LBA's span a wide range from small to large and few too many resources. This underscores the need to not assume that any BA (or LBA) that performs or supports any BA function or part of a BA function is necessarily critical to BES reliability. Please provide the analysis and justification to how these entities fit into the BA requirement as stated in 1.14. If it is the intent of the SDT to capture the generation within the balancing functions of a BA, the SDT has that covered by Criteria 1.15. Q3: Disagree, While we agree with the general requirement of R1, we do not agree with certain aspects of Attachment 1 - Critical Asset Criteria, as discussed in responses to previous questions, above. Q4: Agree Q5: No, The implementation plan is clear on entities that either have in the past, identified they have CA's or have not ever identified CA's. The issue is present that what happens when an entity has only identified a control center as being a CA. But now they have identified a cranking path or Blackstart generator as being a CA. It is recommended that if non like items are identified as a CA, that the entity is given 24 months to become compliant. This will allow the entity enough time since they are now in an area that they may have not dealt with in the past.

Voter	Entity	Segment	Vote	Comment
				Q6: No, See question 5.

Response: Thank you for your comments.

Q1: The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology throughout North America.

Q2: Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize.

Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." It is appropriate to refer to an industry approved and NERC BOT approved standard in a guidance document, even if it has not been accepted at FERC.

Q3: Please refer to response to Q2 above.

Q4: Thank you.

Q5: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Q6: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Steven Grego	MEAG Power	5	Negative	MEAG supports the APPA's comments submitted to the NERC CIP standard drafting team.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Don Schmit	Nebraska Public Power District	5	Negative	NPPD comments are addressed by comments submitted through APPA.
Response: Thank you for your comments. Please refer to the response to comments document.				
Patricia A. Lynch	NRG Energy, Inc.	5	Negative	Pertaining to CIP-002-4 R1, the following need to be addressed in Attachment 1: 1.1 - Add capacity factor as a qualifier for exclusion below an established low threshold. 1.3 - Mandate coordination/approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. These classifications and approvals need to take into consideration 5 year forecasts for planning and budgeting purposes.. 1.5 - TOP needs to define the cranking path in restoration plan to the affected entities to adequately secure these restoration paths.. 1.9 - Please explain FACTS - need definition 1.10 - Need coordination between TOP & GO to identify critical assets. 1.15 - How is the 1500 MW aggregate determined? Is it an aggregate of generator name plates or the sum of controllable megawatts between a unit's high and low limits? General: Attachment 1 needs to have defined terms for capability, plant, control center Requirement 2 needs to clarify the following items: 1) Need Clarification on routable path, discrete links and serial connections as it pertains to CIP-002-3 R3: Is a device considered to communicate outside the ESP using routable protocol if ANY portion of the communications path uses routable protocol? 2)Need clarification concerning shared assets. Does it mean shared between a single device or same device on a network? 3)R2 states that only shared cyber assets for a group of generating units at a single location identified in Attachment 1 criteria 1.1, namely the 1500 MWs brightline, that could impact reliable operation, should be considered. Does this cyber asset identification only include assets meeting criteria 1.1 and therefore exclude any cyber assets utilized for reliable operation of a designated critical asset such as a single blackstart resource? Please

Voter	Entity	Segment	Vote	Comment
				provide clarification in this requirement.

Response: Thank you for your comments.

Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Item 1.9 – FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability."

Item 1.10 – The assets would be identified by the asset owners. It is agreed that communication between GOs and TO/TOPs will be required.
Item 1.15 – This is the aggregate highest rated net Real Power capability output of all generation under dispatch/control.

At this time, the SDT is choosing not to add "capability," "plant," or "control center" to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.

The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1.

Colin Anderson	Ontario Power Generation Inc.	5	Negative	Section 4.2.1 in previous versions of CIP-002 used to exempt "Facilities regulated by the US Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission". This exemption has been removed in draft CIP-002 version 4. Canada has its own laws and regulations and all nuclear facilities within Canada are covered by them. The CNSC regulates the complete nuclear site and we are of the strong opinion that a single regulator (CNSC) should have jurisdiction over the full operating island of nuclear assets due to the over-riding concern for nuclear safety issues. The cyber security standards should be under the jurisdiction of the CNSC in Canada. As such, Section 4.2.1 in CIP-002-4 should continue to exempt the

Voter	Entity	Segment	Vote	Comment
				following; "Facilities regulated by the Canadian Nuclear Safety Commission".
Response: Thank you for your comments. The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
Richard Kinas	Orlando Utilities Commission	5	Negative	comments submitted through online comment form
Response: Thank you for your comments. Please refer to the response to comments document.				
Richard J. Padilla	Pacific Gas and Electric Company	5	Negative	While we understand the need to have a consistent application across the BES, the brightline methodology does not provide enough flexibility to determine what is a critical asset. We recommend an additional attempt to develop guiding principles for determining critical facilities without unilateral declarations on what is critical. The standard development process is still too much in the infant stage with vague definitions. Flexibility is needed to allow entities to develop their CIP responses to meet their critical needs.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.				
Tim Hattaway	PowerSouth Energy Cooperative	5	Negative	Primary concern that a blanket statement of "all blackstart resources" would effectively incentivize utilities to write out blackstart resources to avoid the protection involved, ultimately decreasing the reliability of the system. Perhaps a better requirement would be blackstart resources identified as primary restoration components in a region's restoration plans.
Response: Thank you for your comments. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.				

Voter	Entity	Segment	Vote	Comment
Jerzy A Slusarz	PSEG Power LLC	5	Negative	Project 2008-06: Cyber Security - Order 706 November, 2010
Response: Thank you for your comments.				
Thomas J. Bradish	RRI Energy	5	Negative	Criteria 1.6 and 1.7 are arbitrary without clarification and in relation to Criteria 1.10. Suggest adding the following clarification to the end of Criteria 1.6 and 1.7: ", unless the Transmission Facilities only provide the generation interconnection required to directly connect generator output to the transmission system." o Criteria 1.6, as modified, should read as follows: "Transmission Facilities operated at 500-kV or higher, unless the Transmission Facilities only provide the generation interconnection required to directly connect generator output to the transmission system." o Criteria 1.7, as modified, should read as follows: "Transmission Facilities operated at 300-kV or higher at stations interconnected at 300-kV or higher with three or more other transmission stations, unless the Transmission Facilities only provide the generation interconnection required to directly connect generator output to the transmission system." Clarifications such as the ones presented above and with respect to Criteria 1.6 and Criteria 1.7 would be unnecessary if the Drafting Team first acknowledged the technical distinction between “generator interconnection facilities” and “transmission facilities.” Without such a distinction, radial generator interconnection facilities are indistinguishable from parallel transmission facilities and, as a result, there are mis-applications of the registration criteria and mis-applications of Reliability Standards such as in the case of the Milford and Cedar Creek wind farms. The Drafting Team should take special aim at avoiding further codification of such technically deficient mis-applications in the CIP Reliability Standards.
Response: Thank you for your comments. Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations.				

Voter	Entity	Segment	Vote	Comment
Bethany Wright	Sacramento Municipal Utility District	5	Negative	After reviewing the proposed version 4 language for CIP-002, R2, the placement of the additional text on generation is confusing. It appears to be trying to accomplish two different purposes. SMUD does not have any objections to the text itself, just the placement. SMUD proposes organizing the requirement as follows: R2. Critical Cyber Asset Identification- Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall review this list at least annually, and update it as necessary. R2.1 For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.1.2 The Cyber Asset uses a routable protocol within a control center; or, R2.1.3 The Cyber Asset is dial-up accessible. R2.2 For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1., the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Additionally, SMUD, as a member of APPA, would like to reflect its support to those CIP-002-4 Standard comments submitted by APPA staff.
Response: Thank you for your comments. Please refer to the response to comments document for responses to APPA comments. Requirement R2 has been changed to clarify the issues presented.				
Glen Reeves	Salt River Project	5	Negative	SRP believes that a bright line assessment methodology for determining Critical Assets is not in the best interest of reliability. This is especially true in the designation of substations and generating facilities. The attributes of these stations and their unique impact on Bulk Electric System reliability must be taken into account. There are several terms and phrases used within Requirement 2 of the proposed Standard that need to be better defined to eliminate ambiguity. These terms are: 1) essential to the operation of the Critical Asset, 2) adversely impact the reliable operation needs to be defined; and, 3) within 15 minutes. We believe the CIP-002-4 implementation plan for newly identified Critical Assets and associated Critical Cyber Assets provides inadequate time. SRP suggests the implementation timeframe be extended to 30 months after the effective date of the Standard.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about (annual) exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. Thank you for your comment. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
George T. Ballew	Tennessee Valley Authority	5	Negative	Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this CIP-002-4 draft. We fully support the standards development process and all the hard work and commitment by the drafting team members. For this draft, we have the following concerns which moved us to cast a Negative vote. Q1: Yes; no comment Q2: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. The language appears to require us to designate “Each” component in the System Restoration plan as CA. Because we currently include at least 2 paths for black start of most generation plants in the system, the proposed language would require the extension of CA designation to a large number of components which otherwise would not be included by other criteria. The flexibility provided by our robust transmission infrastructure and the large number of black start capable plants serves to ensure reliable operation of the BES, but designating as a CA each component that could participate in the total paths possible doesn’t seem consistent with the intent of the standard. Recommendation: Revise language to allow entities to limit CA designation to those components participating in the primary black start path. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3. There isn’t a clear definition of the term “directly connected.” Without this definition there are many way to interpret this requirement. Is this language meant to describe a facility where the substation is co-located with a generation facility? Also, does the language this mean total loss of substation or only partial? Recommendation: For the purpose of this

Voter	Entity	Segment	Vote	Comment
				standard revise language to clearly define "directly connected." Q3: Yes; no comment Q4: Yes; no comment Q5: abstain Q6: abstain
Response: Thank you for your comments. Item 1.4 – The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any transmission Facility that, if lost, would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include the partial or total loss of a substation.				
Karl Bryan	U.S. Army Corps of Engineers Northwestern Division	5	Negative	The Standards Drafting Team has chosen to be prescriptive in determining Critical Assets. The Responsible Entity is responsible for identifying Critical Assets and FERC directed NERC to provide additional guidance in helping the Responsible Entity determine Critical Assets and for NERC to maintain flexibility for the Responsible Entity in the determination of Critical Assets. The prescriptive nature of the approach being used in the Ver 4 CIP Standard appears to be taking the responsibility of determining Critical Assets away from the Responsible Entity and the lack of flexibility may eliminate or preclude a system or component from being identified as a Critical Asset.
Response: Thank you for your comments. Regarding the directives for external review and guidance in the FERC Order, the SDT believes the criteria in Attachment 1 are in response to FERC Order 706 paragraph 329. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This "bright-line" approach removes the variability of entity defined methodologies that would prompt the need for external review.				
Linda Horn	Wisconsin Electric Power Co.	5	Negative	1. When reviewing the mapping document posted with the proposed CIP-002-4 standard, do you believe that the proposed standard will lead to an improvement in reliability when compared to the standard it proposes to replace? 1 Yes 0 No Comments: We understand that the errata, which removes discussion of the "risk-based assessment methodology" from the

Voter	Entity	Segment	Vote	Comment
				proposed CIP-002-4 standard, would also apply to the mapping document. We appreciate the bright-line clarification to ensure consistent identification of Critical Assets throughout the industry. 2. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: We suggest that the functional entities Planning Coordinator and Transmission planner be added to the applicability section. Feedback on specific criteria as follows: 1.1, We request clarification on the phrase “single plant location”. This phrase is not defined and it is not clear what level of proximity of generators would be considered a “single plant location”. Rather than discuss this in terms of geography (location), we feel it would be better to discuss in terms of “Each group of generating units (including nuclear generation), operated using common cyber control systems other than the Control Centers identified in 1.14 and 1.15, with an aggregate...”. 1.3, We suggest the wording: “Each generation facility designated by the Planning Coordinator or Transmission Planner as required to avoid one or more reliability criteria violations”. 1.4, The blackstart units deemed critical should be only those identified by the Transmission Operator to meet the minimum critical blackstart requirement. The resulting suggested wording would be: “Each Blackstart Resource identified in the Transmission Operator’s restoration plan required to meet the minimum critical blackstart requirement”. 1.8, We suggest the wording: “Transmission Facilities at a single location that the Planning Coordinator or Transmission planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations”. 1.9, We suggest similar wording: “...unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations”. 1.11, We suggest the following wording: “Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements”. 1.12, We suggest the following wording: “...unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed”. 1.14, We suggest this be made consistent with 1.15, i.e. “Each control center, or backup control center, used to perform the functional obligations

Voter	Entity	Segment	Vote	Comment
				of the Reliability Coordinator, Balancing Authority, or Transmission Operator". 1.16, We suggest the following wording: "Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include". 3. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification - Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 - Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: 4. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement. 1 Agree 0 Disagree Comments: Although we agree with the proposed Requirement R2, We are concerned that the document "CIP-002-4 Cyber Security - Critical Cyber Asset Identification: Rationale and Implementation Reference Document" actually appears to provide more rationale and guidance on Critical Assets than Critical Cyber Assets. 5. Do you agree with the proposed implementation plan for the Version 4 standards? If not, please explain and provide specific suggestions for improvement. 1 Yes 0 No Comments: 6. Do you agree with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities? If not, please explain and provide specific suggestions for improvement. 0 Yes 1 No Comments: We believe that it would be better to simply have a uniform 18 month

Voter	Entity	Segment	Vote	Comment
				implementation deadline for newly identified CCAs rather than have different timelines for different requirements. This will simplify reporting and streamline efforts to become fully compliant. We understand that nuclear timelines are subject to NRC requirements and the necessity of accomplishing some tasks only during refueling outages appropriately dictates a separate schedule for them.

Response: Thank you for your comments.

Q2. Since there is no Requirement that applies to the Planning Coordinator or the Transmission Planner, it is not appropriate to include them in the Applicability section.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.

Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology. The present wording is appropriate. This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Voter	Entity	Segment	Vote	Comment
Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. Q4. Thank you for your comments. The SDT will reexamine the guidance document. Q5. Due to the limited scope of version 4, the SDT is only making conforming changes to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.				
Leonard Rentmeester	Wisconsin Public Service Corp.	5	Negative	WPS and UPPCO believe that a bright line criteria as proposed by the ballot will improve the reliability and safety of the BES. However, changes as provided by MRO's NSRS need to be incorporated into the proposed standard to eliminate the potential for arbitrary application and capricious enforcement of the standard.
Response: Thank you for your comments. Please refer to the response to comments document.				
Liam Noailles	Xcel Energy, Inc.	5	Negative	Please see our comments submitted during the concurrent comment period.
Response: Thank you for your comments. Please refer to the response to comments document.				
Edward P. Cox	AEP Marketing	6	Negative	Overall, AEP is supportive of the efforts and the general concepts of this draft; however, there are a few refinements that will enhance the requirements and remove ambiguity. AEP encourages the SDT to consider the items below in a future draft of the standard: AEP would contend that there are regional differences that would be relevant to determine a MW threshold for generators. We support the concept that was contained in the last draft that made the determination based on the capacity reserves.

Voter	Entity	Segment	Vote	Comment
				However, the prior language would need to be revisited to ensure that value was fixed for a period of time. In addition, requirement 2.2 uses the term control center (also used in attachment 1) that is not a NERC defined term. This will introduce ambiguity to implementation. There has been ongoing confusion regarding the difference between "control centers" and "control rooms." We do not believe that a "control room" at a power plant or a substation would be considered a "control center." There is language in the NERC Security Guideline for Electricity Sector: Identifying Critical Assets document that the SDT should consider and incorporate into the NERC Glossary. Net real power capability testing is defined in MOD-024 standards that have yet to be FERC approved. Furthermore, not all of the regions have defined the parameters for the capability testing.
Response: Thank you for your comments. Item 1.1 - In prior versions we had wording about reserve sharing for the threshold. We received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. We did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. At this time, the SDT is choosing not to add "control center" to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. CIP-002-4 does not require net real power capability testing.				
Jennifer Richardson	Ameren Energy Marketing Co.	6	Negative	1. (a) The proposed bright line criteria are not based on any studies or performance testing. (b) The proposed bright line criteria do not address proximity to load centers or the impact to system flows or voltages in those load centers. (c)Also, we believe that impact on the BES should be evaluated for the Critical Asset using the performance requirement contained in the existing mandatory standards. This would provide consistency between CIP-002 and other standards. In this regard, we suggest that for the facilities identified in the bright line criteria, perform powerflow and stability simulations to assess the impact to the BPS of the outage of these facilities, similar to the tests performed for TPL-003 and 004. If there is an impact (that is not meeting the performance criteria), then the facility is to be considered as critical. If there is no such impact, then the facility is not be considered as critical. If there is a concern for a multi-prong attack, then similar reliability assessment should be performed for such scenarios. (d)Further, the bright line criteria will include many

Voter	Entity	Segment	Vote	Comment
				more facilities as critical assets with minimal to no improvement to reliability and would require significant resource commitment to meet the proposed implementation schedule. 2. We offer some comments/suggestions and also have some questions/comments to the bright line criteria (Attachment 1): (a) The term “Facilities” should be changed to “substations and switchyards” throughout Attachment 1 as NERC glossary of terms include “lines” in the definition also. Is it SDT’s intention to include hundreds of miles of lines as critical asset? (b) The term “single station location” and “single plant location” used throughout Attachment 1 need to be defined to avoid confusion whether a single location mean one building or several buildings or stations within a defined geographical boundary or a fenced area. (c) Specific comments to Attachment 1 : 1.1 - Are there any reliability impact studies to support 1500 MW? We believe that several events larger than this number have occurred and the BES has performed as designed, without any loss of load, or significant impact on reliability. 1.6 - We disagree that all transmission facilities operated at 500 kV or greater are “critical”. Again, system studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.7 - We disagree that all transmission facilities that are operated at 300 kV or above and are interconnected with three or more transmission substations are “critical. System studies should be conducted to take into account the impact that the asset has on the reliable operation of the BES before determining that an asset is a Critical Asset. 1.8 - Wording for this criterion should be changed to “Transmission substations and switchyards that the Planning Coordinator or Transmission Planner designates that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL). This change would make this criterion consist with FAC-010/FAC-014. 1.12 - We believe that the criterion reads ok, but the rationale document for this criterion implies that purpose of SPS/RAS is to prevent disturbance that would result in excursion beyond IROLs. This may not be true in all cases. 1.13 - Wording for this criterion should be changed to “Common control system(s) capable of performing automatic load shedding of 300 MW or more with a single operation”. 1.15 - Same comments as for 1.1 above. 1.16 - Wording for this criterion should be changed to “Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include.” 3. CIP-002-4, R2 : (a) The word “associated” could mean anything to do with a Critical Assets

Voter	Entity	Segment	Vote	Comment
				which is too broad of a term and needs to be defined to avoid confusion. (b)The phrase "could adversely impact the reliable operation" is unclear and vague. What magnitude of "adverse impact" should be considered? Also what is being defined as the Reliable Operation? This phrase should be more clearly defined, otherwise it could introduce different interpretations in the compliance audits. 4. The implementation plan is very confusing.

Response: Thank you for your comments.

(1) The SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. Significant feedback from the industry was the need to simplify the Critical Asset identification approach. We welcome your suggestions for improvement to the criteria. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The results of the recent NERC data request were used to assist the team in developing the criteria in Attachment 1. Bright-line criteria by its very nature may overreach in some areas and under-reach in others, with the end result being a more protected system on average.

The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry.

2. a) A transmission Line can be considered a Critical Asset if it meets the criteria in Attachment 1. It would then be evaluated for possible Critical Cyber Assets, which would be afforded the cyber security protection outlined in CIP-003 to CIP-009. It is not the Critical Asset that falls under CIP-003 to CIP-009, but the Critical Cyber Asset.

b) The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.
c) Item 1.1 - In prior versions we had wording about reserve sharing for the threshold. We received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. We did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

Items 1.6 and 1.7 – You propose to add the criteria that the Responsible Entity can determine through a risk-based evaluation that destruction, degradation or unavailability of certain assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. The SDT does not feel that a power flow analysis (impact-based or risk-based) may lead to a consistent application of the

Voter	Entity	Segment	Vote	Comment
criteria, due to the numerous factors which can impact substation power flows. Such a study would need to be rigorously defined for the industry. We thank you for your proposal and will take it under consideration for future revisions. Criterion 1.7 has been reworded to "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations." Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.15 –In the development of this criterion, the drafting team used 1500 MW as a bright-line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections. Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot. (3) The phrase "adversely impact" limits the scope of the evaluation of Critical Cyber Assets to those that can affect the reliable operation of 1500MW or more of generation at a single plant location. (4) The implementation plan is a modification of the implementation plan for version 3 of the CIP standards.				
Brian Ackermann	Associated Electric Cooperative, Inc.	6	Negative	please review submitted comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Brenda S. Anderson	Bonneville Power Administration	6	Negative	Please refer to BPA comments submitted during the formal comment period on 10/26/10
Response: Thank you for your comments. Please refer to the response to comments document.				
Brenda Powell	Constellation Energy	6	Negative	Constellation Energy Commodities Group could vote affirmative in the next ballot if specific comments submitted on the Comment Form for Project

Voter	Entity	Segment	Vote	Comment
	Commodities Group			2008-06-Cyber Security 706 were successfully addressed (also submitted 11/3/10).
Response: Thank you for your comments. Please refer to the response to comments document.				
Louis S Slade	Dominion Resources, Inc.	6	Negative	Dominion conceptually supports bright line criteria for determining critical assets. However, we cannot vote in favor at this time because we believe that changes are needed in Table 2 that recognize the implementation for infrastructure (physical and electronic security) should be equal to, or longer than, that required for training. We also believe that the bright line criteria for generation control center needs further effort. Please see more specific comments submitted using the NERC comment link for this project.
Response: Thank you for your comments. Please refer to the response to comments document.				
Larry W. Rodriguez	Entegra Power Services	6	Negative	There has been no consideration for "small shops" that will have an extreme financial impact. In addition, the only cyber security breach possibility is from Control Room employees, which is so very unlikly!
Response: Thank you for your comments. Cost is only one of many issues that must be considered in the cyber security of the BES. The set of CIP cyber security standards (CIP-002 to CIP-009) is a holistic approach to cyber security protection that applies to both internal and external threats.				
Terri F Benoit	Entergy Services, Inc.	6	Negative	Switchyards serving nuclear facilities should not be automatically classified as critical assets. The fact that a BES switchyard serves a nuclear facility should not in itself qualify the switchyard as a critical asset. While nuclear units and their support facilities may qualify as critical assets under a separate set of criteria, they should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability. All blackstart units and associated cranking paths should not be automatically classified as critical assets. Blackstart units may be useful in the restoration of the BES following a large scale outage, but they are not necessarily essential to the reliability of the BES under normal operation. Blackstart units should not automatically be designated as critical to the BES without some measure of the impact of the loss of the facility on BES reliability.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2, "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." The SDT feels that these units must be classified as Critical Assets. It should be noted that not all blackstart generators are Blackstart Resources.				
Richard L. Montgomery	Florida Municipal Power Agency	6	Negative	FMPA commends the SDT on making significant headway on the version 4 standards. However, there are significant additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified. Please see FMPA's comments submitted through the formal comment process for more specific detail and proposed alternatives.
Response: Thank you for your comments. Please refer to the response to comments document.				
Thomas E Washburn	Florida Municipal Power Pool	6	Negative	Please see APPA's comments
Response: Thank you for your comments. Please refer to the response to comments document.				
Paul Shipps	Lakeland Electric	6	Negative	Several additional improvement that should be made to make the criteria of Attachment 1 less arbitrary and that truly measures those assets that can have an Adverse Reliability Impact. Also, the standard is still unclear in several areas, such as how to identify CCAs at a substation if a substation is determined to be a CA that needs to be clarified.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.				

Voter	Entity	Segment	Vote	Comment
Eric Ruskamp	Lincoln Electric System	6	Negative	Please review the comments submitted by the MRO's NERC Standards Review Subcommittee for LES' reasons for a negative ballot.
Response: Thank you for your comments. Please refer to the response to comments document.				
Brad Jones	Luminant Energy	6	Negative	Luminant Energy Company LLC (Luminant Energy) thanks the Standard Drafting Team (SDT) for their work on the NERC CIP Cyber Security Standards and for the opportunity to provide input into the standards development process. Although Luminant Energy has voted "Negative" on the current draft standard, Luminant Energy supports the SDT goal of completing the revision of CIP-002-4 by the end of December 2010, and believes with some modification to the Attachment 1 Criteria, the goal is still achievable. Specifically, Luminant Energy is concerned that Criteria 1.3 has no defined basis for determining the reliability need of a generation Facility. As written, the Planning Coordinator or Transmission Planner could use any basis, or conversely, no basis, for designating a generation Facility as required for reliability purposes. For Criteria 1.8, 1.9, and 1.12, the SDT has appropriately used the violation of an Interconnection Reliability Operating Limit (IROL) as the basis for determining the reliability need of transmission Facilities. Luminant Energy believes this same basis is appropriate for application to generation Facilities in Criteria 1.3, and offers the following language for consideration by the SDT: 1.3 "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes, by demonstrating that the generation facility, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs)."
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."				
Jeffrey M Keebler	Madison Gas and Electric Co.	6	Negative	The below are outstanding issues that the SDT should address before the next ballot. Comments are in line with the Unofficial Comment Form for Project 2008-06. Q1: No, If a brightline is used, it removes all engineering analysis the entity is currently performing with the current CIP-002-3 methodology. This may

Voter	Entity	Segment	Vote	Comment
				bring in or remove assets for this Standard. A brightline approach may be useful to a smaller entity but may not be in the best interest to larger entities. The SDT should consider a brightline with a MW threshold for physical unit size or MW loads for control centers, see comments below. Q2: Yes, Criteria number 1.5; Based on the Rationale Document, please clarify that Facilities within the Cranking Paths will be assigned the Critical Asset identification up to the point where multiple path options exist. Criteria number 1.13; Based on the Rationale Document, please clarify that the 300 MW level applies to a single common control system and not multiple like systems such as those installed for UFLS protection (multiple identical or similar individual, but independent, relays that may shed 300 MW's or more in aggregate, but individually shed less than 300 MW). Criteria number 1.14; Based on the Rationale Document, every RC, BA, and TOP's control center, control system, backup control center and backup control system is Critical due to EOP-008. EOP-008-0 is the FERC approved Standard for US entities. The purpose of EOP-008-0 is: "Each reliability entity must have a plan to continue reliability operations in the event its control center becomes inoperable". The SDT quoted EOP-008-1 in the Rational Document, which is not FERC approved. The SDT needs to consider this when writing a continental wide Standard. The phrase in the Rationale Document: "While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets", is unjustified. Assuming a BA controls no critical assets qualified as such by other criteria, a BA that, in aggregate, controls relatively small amounts of real and/or reactive power clearly has less of an effect on reliability than a BA that controls relatively large amounts of such resources. Indeed, the fact that "size matters" is recognized by Criteria 1.1, 1.2, 1.6, 1.7, 1.13, and 1.15. Criterion 1.14 should be modified to recognize this conclusion by including relevant quantitative thresholds. Thresholds that were proposed in CIP-010 Criteria 1.13 and 1.14 would be reasonable. In any event, the thresholds for the BA control center or control system should be no more inclusive than those used to qualify the individual assets controlled by the BA. To complicate matters, presently there are 28 Local Balancing Authorities (LBA's) that are part of the Midwest ISO BA Area (JRO00001). These entities do not perform all the BA functional obligations as stated in the Rationale Document (the MISO BA performs the majority of BAL-001 through BAL-005). Furthermore, the scopes of operation of the LBA's span a wide range from small to large and

Voter	Entity	Segment	Vote	Comment
				few too many resources. This underscores the need to not assume that any BA (or LBA) that performs or supports any BA function or part of a BA function is necessarily critical to BES reliability. Please provide the analysis and justification to how these entities fit into the BA requirement as stated in 1.14. If it is the intent of the SDT to capture the generation within the balancing functions of a BA, the SDT has that covered by Criteria 1.15. Q3: Disagree, While we agree with the general requirement of R1, we do not agree with certain aspects of Attachment 1 - Critical Asset Criteria, as discussed in responses to previous questions, above. Q4: Agree Q5: No, The implementation plan is clear on entities that either have in the past, identified they have CA's or have not ever identified CA's. The issue is present that what happens when an entity has only identified a control center as being a CA. But now they have identified a cranking path or Blackstart generator as being a CA. It is recommended that if non like items are identified as a CA, that the entity is given 24 months to become compliant. This will allow the entity enough time since they are now in an area that they may have not dealt with in the past. Q6: No, See question 5.

Response: Thank you for your comments.

Q1: The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology throughout North America.

Q2: Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize.

Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." It is appropriate to

Voter	Entity	Segment	Vote	Comment
refer to an industry approved and NERC BOT approved standard in a guidance document, even if it has not been accepted at FERC. Q3: Please refer to response to Q2 above. Q4: Thank you. Q5: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset. Q6: The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Daniel Prowse	Manitoba Hydro	6	Negative	Please see comments submitted by Manitoba Hydro in the formal comment period.
Response: Thank you for your comments. Please refer to the response to comments document.				
Joseph O'Brien	Northern Indiana Public Service Co.	6	Negative	As NIPSCO understands the current set of CIP standards CIP-002-4 - CIP-004-4 & CIP-006-4 - CIP-009-4 it appears that each of the proposed standards needs to be corrected to modify the purpose section, which references the entire set of standards CIP-002-4 - CIP-009-4 when in reality CIP-005-4 does not yet exist and is not being balloted in at this time. In addition CIP-003-4 R1, R2 make reference to the entire set of version 4 standards, which would also include the unapproved CIP-005-4. The unapproved CIP-005-4 is specifically identified as a compliance requirement within CIP-006-4 R2.2 and CIP-007-4 R7. The primary concern is that the industry is being asked to ballot on a set of standards that references a standard that does not yet exist. There is also concern for future applicability concerns in regards to effective dates with CIP-005-4 and implementation date overlap conditions that could occur when CIP-005-4 goes to ballot again and potentially get approved. This is a straightforward correction to the version 4 standards and would most easily be resolved by proposing a new CIP-005-4 that simply updates the versioning information within the standard in the same approach that was taken for CIP-003-4 - CIP-004-4 & CIP-006-4 - CIP-009-4. In CIP-002 Version 4 under Applicability we're not sure why NERC is listed. At the very least this should

Voter	Entity	Segment	Vote	Comment
				be replaced by ERO however it's still not clear how this entity fits in with the Functional Model.
Response: Thank you for your comments. The following information was provided with the posting of the CIP Version 4 standards: *(CIP-005-4 - Cyber Security — Electronic Security Perimeter is posted separately, with a set of proposed revisions for Urgent Action under Project 2010-15. If CIP-005-4 is not approved as an Urgent Action, it will be returned to this set of CIP standards.)* As for listing NERC in the Applicability section, NERC has historically been listed in this section for the CIP body of standards.				
Alan R. Johnson	NRG Energy, Inc.	6	Negative	Pertaining to CIP-002-4 R1, the following need to be addressed in Attachment 1: 1.1 - Add capacity factor as a qualifier for exclusion below an established low threshold. 1.3 - Mandate coordination/approval process between the Transmission Planner and entity that have been designated critical by the Transmission Planner. These classifications and approvals need to take into consideration 5 year forecasts for planning and budgeting purposes.. 1.5 - TOP needs to define the cranking path in restoration plan to the affected entities to adequately secure these restoration paths.. 1.9 - Please explain FACTS - need definition 1.10 - Need coordination between TOP & GO to identify critical assets. 1.15 - How is the 1500 MW aggregate determined? Is it an aggregate of generator name plates or the sum of controllable megawatts between a unit's high and low limits? General: Attachment 1 needs to have defined terms for capability, plant, control center Requirement 2 needs to clarify the following items: 1) Need Clarification on routable path, discrete links and serial connections as it pertains to CIP-002-3 R3: Is a device considered to communicate outside the ESP using routable protocol if ANY portion of the communications path uses routable protocol? 2)Need clarification concerning shared assets. Does it mean shared between a single device or same device on a network? 3)R2 states that only shared cyber assets for a group of generating units at a single location identified in Attachment 1 criteria 1.1, namely the 1500 MWs brightline, that could impact reliable operation, should be considered. Does this cyber asset identification only include assets meeting criteria 1.1 and therefore exclude any cyber assets utilized for reliable operation of a designated critical asset such as a single blackstart resource? Please

Voter	Entity	Segment	Vote	Comment
				provide clarification in this requirement.

Response: Thank you for your comments.

Item 1.1 – The SDT debated whether to include capacity factor in this criterion. The reason we ultimately chose not to include capacity factor is twofold. First, there is no consistent method to select an appropriate capacity factor, and low capacity factor units may be critical to the system at peak load conditions. Second, there was concern that some units might fall below the line during major outage periods, taking them off the Critical Asset list one year and putting them back on the list the next year.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

Item 1.9 – FACTS is defined by IEEE as "Alternating Current Transmission Systems incorporating power electronics-based and other static controllers to enhance controllability and power transfer capability."

Item 1.10 – The assets would be identified by the asset owners. It is agreed that communication between GOs and TO/TOPs will be required.

Item 1.15 – This is the aggregate highest rated net Real Power capability output of all generation under dispatch/control.

At this time, the SDT is choosing not to add "capability," "plant," or "control center" to the NERC Glossary. We feel defining these terms under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. These terms are used in other approved NERC standards already in effect.

The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1.

James D. Hebson	PSEG Energy Resources & Trade LLC	6	Negative	Please see PSEG companies' comments filed separately. The PSEG Companies will change the vote to affirmative if the comments are adequately addressed by the drafting team.

Response: Thank you for your comments. Please refer to the response to comments document.

Trent Carlson	RRI Energy	6	Negative	Criteria 1.6 and 1.7 are arbitrary without clarification and in relation to Criteria 1.10. Suggest adding the following clarification to the end of Criteria 1.6 and 1.7: ", unless the Transmission Facilities only provide the

Voter	Entity	Segment	Vote	Comment
				generation interconnection required to directly connect generator output to the transmission system." o Criteria 1.6, as modified, should read as follows: "Transmission Facilities operated at 500-kV or higher, unless the Transmission Facilities only provide the generation interconnection required to directly connect generator output to the transmission system." o Criteria 1.7, as modified, should read as follows: "Transmission Facilities operated at 300-kV or higher at stations interconnected at 300-kV or higher with three or more other transmission stations, unless the Transmission Facilities only provide the generation interconnection required to directly connect generator output to the transmission system."
Response: Thank you for your comments. Item 1.6 –The drafting team believes all Transmission Facilities operated at 500 kV or higher do not require any further qualification for their role as components of the backbone on the Interconnected BES. Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations.				
Mike Hummel	Salt River Project	6	Negative	SRP believes that a bright line assessment methodology for determining Critical Assets is not in the best interest of reliability. This is especially true in the designation of substations and generating facilities. The attributes of these stations and their unique impact on Bulk Electric System reliability must be taken into account. There are several terms and phrases used within Requirement 2 of the proposed Standard that need to be better defined to eliminate ambiguity. These terms are: 1) essential to the operation of the Critical Asset, 2) adversely impact the reliable operation needs to be defined; and, 3) within 15 minutes. We believe the CIP-002-4 implementation plan for newly identified Critical Assets and associated Critical Cyber Assets provides inadequate time. SRP suggests the implementation timeframe be extended to 30 months after the effective date of the Standard.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.				

Voter	Entity	Segment	Vote	Comment
The phraseology you are concerned about (annual) exists in the existing CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version Thank you for your comment. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Marjorie S. Parsons	Tennessee Valley Authority	6	Negative	Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this CIP-002-4 draft. We fully support the standards development process and all the hard work and commitment by the drafting team members. For this draft, we have the following concerns which moved us to cast a Negative vote. Q1: Yes; no comment Q2: 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. The language appears to require us to designate “Each” component in the System Restoration plan as CA. Because we currently include at least 2 paths for black start of every generation plant in the system, the proposed language would require the extension of CA designation to a large number of components which otherwise would not be included by other criteria. The flexibility provided by our robust transmission infrastructure and the large number of black start capable plants serves to ensure reliable operation of the BES, but designating as a CA each component that could participate in the total paths possible doesn’t seem consistent with the intent of the standard. Recommendation: Revise language to allow entities to limit CA designation to those components participating in the primary black start path. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3. There isn’t a clear definition of the term “directly connected.” Without this definition there are many way to interpret this requirement. Is this language meant to describe a facility where the substation is co-located with a generation facility? Also, does the language this mean total loss of substation or only partial? Recommendation: For the purpose of this standard revise language to clearly define “directly connected.” Q3: Yes; no comment Q4: Yes; no comment Q5: abstain

Voter	Entity	Segment	Vote	Comment
				Q6: abstain
Response: Thank you for your comments. Item 1.4 – The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term, nor is it used in EOP-005-2. A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources. Item 1.10 – The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. That might include the partial or total loss of a substation.				
David F. Lemmons	Xcel Energy, Inc.	6	Negative	Please see our comments submitted during the concurrent comment period.
Response: Thank you for your comments. Please refer to the response to comments document.				
James A Maenner		8	Negative	The Applicability for CIP-002-4 seems to cast a wide enough net to find some entity responsible for determining assets as critical. The problem is that most of those listed in Section 4 have no ability or expertise to study or determine the criticalness of an asset on the BES. Ultimately, the identification of critical assets should be the responsibility of the Planning Coordinator or Transmission Planner with a notification (and explanation) to the critical asset owner who then creates the list of associated Critical Cyber Assets and performs all necessary steps to satisfy Standards CIP-003 through 009. I noticed NERC and the RE on the list. Is there a process for independent monitoring and auditing of those entities? Bullet 1.8 of Attachment 1 should identify the TP or PC as responsible.
Response: Thank you for your comments. The burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. This is consistent with FERC order 706.				

Voter	Entity	Segment	Vote	Comment
The Compliance Monitoring and Enforcement section addresses NERC and the RE. Item 1.8 – According to FAC-014-2, IROLs are established by Transmission Operators, Transmission Planners, and Planning Authorities. The Reliability Coordinator ensures that IROLs are established and are consistent with its methodology.				
Nicholas Lauriat	Network & Security Technologies	8	Negative	The term "risk-based assessment methodology" still appears in the last sentence of R3.
Response: Thank you for your comments. That reference will be removed in the posting for the next ballot.				
Jim R Stanton	SPS Consulting Group Inc.	8	Negative	Critical Asset Criteria 1.3 states: "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." Here, reliability purposes is not defined so the criteria is intrinsically ambiguous, which will likely trigger rounds of interpretation requests. Also, Transmission Planners and Planning Coordinators are not uniformly independent. Non-independent entities, through the application of this criteria, could designate selected competitors as "required for reliability purposes" and do so, as written, without supporting studies and independent affirmation of the designation. Hence, the dramatic costs of compliance with CIP standards will be imposed on competitors, increasing their costs and blunting competition. This criteria fails the SAR condition that states: "A reliability standard shall not give any market participant an unfair competitive advantage." This criteria clearly gives Transmission Planners and Planning Coordinators an unfair competitive advantage. If the criteria is to remain in subsequent revisions, then it should also say that such designations will be supported by independently confirmed studies showing the need for the reliability designation, and subsequent exposure to the CIP standards.
Response: Thank you for your comments. Item 1.3 – The burden for identifying Critical Assets is still the Responsible Entity that is the asset owner. There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability. This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, then that unit must be classified as a Critical Asset. If an entity feels that they have an asset that has been unjustly classified as "required for reliability reasons," there are appeals processes that can be used.				
James D Burley	Midwest Reliability	10	Negative	We do not see any added value in Requirement R1. This requirement requires the reponsible entity to develop a list of its critical assets and then

Voter	Entity	Segment	Vote	Comment
	Organization			from this list, requriement R2 requires the responsible entity to develop a list of critical cyber assets for each identified critical asset. We believe this methodology is flawed. A critical cyber asset may exist at a location not deemed a critical asset.We believe this is a serious flaw in the current standard and the suggest revision does nothing to remedy it.We recommend the drafting team write the requirment so the registered entities simply identify critical cyber assets.
Response: The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues.				
Larry D Grimm	Texas Reliability Entity	10	Negative	(1) Texas RE supports the addition of specific criteria for identifying Critical Assets, as shown in Attachment 1 of this draft. (2) In R3, the reference to "risk-based assessment methodology" is a carry-over from the prior version of CIP-002, and it no longer applies in this version of the standard. (3) In Attachment 1, items 1.14 and 1.15, the term "control center" should be defined or more specifically characterized in order to provide guidance as to exactly what facilities are included. (4) In section 1.3, Compliance Monitoring and Enforcement Processes, "Periodic Data Submittal" should be added to the list, because it is a process that will be useful in monitoring this revised standard.
Response: Thank you for your comments. 1) Thank you. 2) That reference will be removed in the posting for the next ballot. 3) At this time, the SDT is choosing not to add "control center" to the NERC Glossary. We feel defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. This term is used in other approved NERC standards already in effect. 4) Thank you for your comments. At this time the SDT is not choosing to add periodic data reporting to the CIP body of standards.				
Louise McCarren	Western Electricity Coordinating Council	10	Negative	We recognize and appreciate the efforts of the drafting team in developing a bright line set of criteria for identifying Critical Assets. This approach will lead to more uniformity and consistency across the continent in the identification of Critical Assets. However, some stakeholders have indicated that the bright line Criteria included in Attachment 1 of CIP-004-2 will lead to fewer Critical Assets being identified than their initial methodology that was required by older versions of CIP-002. We encourage the drafting team to review the thresholds for identifying Critical Assets to ensure that they are appropriate. We also believe a similar effort in identifying a bright

Voter	Entity	Segment	Vote	Comment
				line criteria for Critical Cyber Assets is necessary. Stakeholders have commented regarding the lack of clarity in the language of Requirement 2 of CIP-002. The language "essential to the operation of the Critical Asset" is subjective and could lead to the same lack of uniformity and consistency in identifying Critical Cyber Assets that drove the changes in identification of Critical Assets. A lack of a uniform and consistent identification of Critical Cyber Assets may prevent the desired level of reliability and security.
Response: Thank you for your comments. While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets in North America will be classified as Critical Assets. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects to correct this phraseology in the next version.				
Jason Shaver	American Transmission Company, LLC	1	Affirmative	ATC agrees the implementation schedule in general, should allow for sufficient time (18 months from effective date; 24 months from FERC approval date) for Category 2 entities to become compliant with CIP-003 through CIP-009. However, we suggest an extension should be allowed for good cause if approved by the Regional Entity.
Response: Thank you for your comments. The suggested modification proposes an exception process to a mandatory standard, and we refer to the discussion on technical feasibility exceptions in the FERC Order. Specifically, the oversight framework which must be in place is summarized in paragraph 222.				
John J. Moraski	Baltimore Gas & Electric Company	1	Affirmative	Affirmative ballot is contingent on successfully addressing specific comments submitted on the Formal Comment Form for Project 2008-06 Cyber Security 706.
Response:Thank you for your comments. Please refer to the response to comments document.				
Chang G Choi	City of Tacoma, Department of Public Utilities, Light Division, dba	1	Affirmative	Tacoma Power has submitted comments during the comment period for Version 4 of the CIP standards. If there is a subsequent future ballot for Project 2008-06, consideration of all submitted comments need to be reflected in such ballot.

Voter	Entity	Segment	Vote	Comment
	Tacoma Power			
Response: Thank you for your comments. Please refer to the response to comments document.				
Christopher L de Graffenried	Consolidated Edison Co. of New York	1	Affirmative	1. New Requirement R1: We request an explicit definition of "annual." In addition, it is not clear whether the "update as necessary" applies to updates to the list during the annual review. The language should be clarified to more definitely express the "update as necessary" to be applicable to the list during the annual review. 2. New Requirement R2: In addition, there is no reason for the parenthetical with the specific inclusion of nuclear generation. It should be removed. 3. Attachment 1/Requirement R2: We suggest the removal of "control system" and "backup control system" in Attachment 1, Part 1.14. These systems should be identified as part of new Requirement R2, Critical Cyber Asset Identification. 4. Attachment 1: Part 1.3 is extremely broad and is under defined. Either delete it or provide additional specificity delineating the limited range of circumstances when a PC or TP may designate a facility as critical. 5. Attachment 1: Part 1.10 uses the phrase "the loss of the assets" without describing the relevant time period. Are these assets losses for a few cycles, for a few minutes, for a few hours or for a few days? We recommend that the conclusion of Part 1.10 state "...would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3 for a period of xx hours (e.g., 24 hours) or more." 6. Implementation Plan: Agreed, so long as an Entity can have access to an exception process with an implementation plan to request additional time due to a large increase in identified assets, without a self-reported violation, within an implementation schedule.
Response: Thank you for your comments. 1) The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects to correct this phraseology in the next version. 2) The parenthetical statement about nuclear generation comes from Attachment 1 criterion 1.1. 3) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the				

Voter	Entity	Segment	Vote	Comment
functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." 4) Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." 5) The phrase "loss of assets" is not limited to any period of time. A trip and a 24 hour outage would both apply. 6) Thank you for your comments.				
Robert Martinko	FirstEnergy Energy Delivery	1	Affirmative	FirstEnergy appreciates the CIP Standard Drafting Team's (SDT) careful consideration of our and other stakeholder feedback during prior comment periods and the SDT's decision to develop the CIP-002-4 bright-line standard. The development of CIP-002-4 and continued use of the CIP-003 through CIP-009 standards brings needed industry consistency in Critical Asset determinations while appropriately building upon prior industry efforts of implementing the CIP standards. FirstEnergy supports CIP-002-4 and is voting AFFIRMATIVE for the standard but believes changes are needed to better clarify Attachment 1. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. Lastly, we encourage the SDT to reconsider its Implementation Plan for the CIP version 4 standards. The Implementation Plan is a 15 page document which is overly complex and difficult to understand. Please refer to FE's comments submitted through the parallel comment period for suggestions for improvement and simplification. The following are FirstEnergy's proposed Attachment 1 changes: 1) Criterion 1.8 currently states "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014. C.) A possible misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say "Transmission Facilities at a single station location ..." not all transmission facilities at a

Voter	Entity	Segment	Vote	Comment
				single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8: "1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL)." The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements" Clarity needed: The term "essential" is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the following change for 1.11: "1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements." 3) Criterion 1.5 currently states "The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist." FirstEnergy suggests replacing the word "multiple" with "two or more" for clarity. 4) Criterion 1.14 currently states "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." FirstEnergy suggests removing the text "control system" and "or backup control system" for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the "control center" then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase "control system" is vague.
Response: Thank you for your comments. Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits				

Voter	Entity	Segment	Vote	Comment
(IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.				
Michael Moltane	International Transmission Company Holdings Corp	1	Affirmative	ITC Votes "Affirmative" on this ballot as we consider it a great improvement over the existing Standard. However, we do have some concerns. Specifically, new CIP-002-4 R2 Critical Cyber Asset Identification- The revisions made are introducing confusion while only identifying the inclusion of Cyber assets with delimited (arbitrarily) time for impact: "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Either a new qualification and characteristic of Critical Cyber Assets is created or the existing characteristics shall be updated to explicitly address the type of Cyber Asset.
Response: Thank you for your comments The requirement refers to shared cyber assets that can have a reliability impact on the group of generating units. This qualifier only includes Critical Assets identified in criterion 1.1. The 15-minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact. We have updated the wording of R2 to clarify the meaning of this phrase.				

Voter	Entity	Segment	Vote	Comment
Michael Gammon	Kansas City Power & Light Co.	1	Affirmative	The bright-lines established by the proposed standard have not been established with a strong engineering basis and do not necessarily reflect a true measure of reliability impact to the bulk electric system. It is recommended to develop a process to determine a true reliability assessment and adjust the bright-line proposed here to a deliberate and supportable definition.
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology.				
Martyn Turner	Lower Colorado River Authority	1	Affirmative	1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. If a multiple path option exists from the Black Start Resource to a Next Start unit, does a Critical Path have to be designated? To clarify, the criteria states "The Facilities comprising the Cranking Paths... up to the point where multiple path option exist." If a transmission owner/operator has multiple paths originating directly at the Black Start Resource, either path could be used as a cranking path. Therefore, neither path would be considered critical. Could this be clarified? 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. 1) Does this includes radial interconnections? This is a question because a 345 kV station could be interconnected to 3 other stations, but one of the interconnections could be a radial 345 kV line connected to a generator. 2) Is there a distance requirement for the interconnection? This is a question because a 345 kV station could be interconnected to 3 other stations, but one of the interconnections could be a 345kV bus connected to another station a few feet away. These questions need to be resolved; otherwise a negative may be considered for these standards in the future ballots.
Response: Thank you for your response Item 1.5 – The point where multiple paths exist in the Cranking Path is the step in the Transmission Operator's restoration plan per EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," where the Transmission Operator can choose between the next Facilities on the BES to energize. Based on your example, neither path would be identified as a Critical Asset.				

Voter	Entity	Segment	Vote	Comment
Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion.				
Saurabh Saksena	National Grid	1	Affirmative	1. First, the proposed standard will lead to an improvement in reliability for entities that are either newly registered or envision new assets coming under their CIP purview. However, based on a preliminary assessment, National Grid anticipates minimal impact of the proposed revisions for National Grid's registered entities. Because National Grid's current risk-based methodology for identifying critical assets is similar to the bright-line criteria proposed in the revision for CIP-002, National Grid's current critical asset list is very inclusive Hence, from National Gird's perspective, the proposed standard will not lead to a significant improvement in reliability with regard to National Grid's facilities because it will not result in a significant increase in the number of assets identified as critical. Second, the proposed revision to the standard aims to replace the existing risk-based methodology with the new bright-line criteria. However, R3 of the proposed standard (reproduced below) still refers to the risk-based methodology. National Grid proposes to delete the reference to the risk-based methodology in R3 for consistency and to reduce the possibility of confusion on the part of senior managers attempting to comply with R3. 2. National Grid proposes to include the class of assets - generation, transmission, and control centers against each criterion in attachment 1. This will help entities to clearly identify which requirements fall under different classes of assets. For example - 1.5 The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist. (Generation, transmission) 3. The standard clearly mentions the documentation required to comply with CIP-002-4 which includes - list of Critical Assets as specified in R1, list of Critical Cyber Assets as specified in R2, and approval records of annual approvals as specified in R3. However, in the Guidance document, Page 7, bullet point 2, second sentence, it states the following - "...Responsible Entity should document all criteria that qualify this asset as a Critical Asset..." National Grid recommends that the drafting team clarifies the

Voter	Entity	Segment	Vote	Comment
				documentation requirements to avoid such discrepancies. If the standards drafting board expects entities to document, and retain documentation, of the criteria that supports the categorization of critical assets, this should be explicitly required by the standard. As the proposed standard is written, the only documentation registered entities must create and retain is the actual list of the assets.
Response: Thank you for your comments. 1) Prior to the next round of balloting, the reference to risk-based methodology in R3 will be removed. 2) The Applicability section of the standard specifies to which NERC Registered Entities the standard applies. All Requirements apply to all Entities listed in the Applicability section. 3) The guidance document has been updated to delete the reference.				
David H. Boguslawski	Northeast Utilities	1	Affirmative	Regarding CIP-002-4 Attachment 1, please consider the following: CIP-002-1 Attachment 1 criterion 1.3 reads: "Each generation facility that the planning coordinator or transmission planner designates as required for reliability purposes". We believe that as stated, this criterion (1.3) is subject to interpretation. Specifically, "for reliability purposes" can be interpreted as "must-run" units, required for black start (although that could be duplicative to criteria 1.4), or as any generator containing BPS elements. Suggest more clearly defining "for reliability purposes" or restating the criterion. The terminology used in the recent NERC data request appeared to be clearer - that is: "Any generation facility that the planning coordinator identifies as Reliability 'must run' assigned units". CIP-002-1 Attachment 1 criterion 1.10 reads: "Transmission facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3." We believe that as stated, this criterion (1.10) could be interpreted to mean not only generators owned by the responsible entity but also those not owned by but interconnected to the Transmission Owner's system. Clarification of criterion 1.3 should serve to clarify criterion 1.10 as well.
Response: Thank you for your comments. Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." Item 1.10 – The SDT agrees that not only generators owned by the Responsible Entity but also those not owned by but interconnected to the				

Voter	Entity	Segment	Vote	Comment
Transmission Owner's system are subject to criterion 1.10.				
Pawel Krupa	Seattle City Light	1	Affirmative	Seattle City Light Subject Matter Expert (SME) supports the changes proposed for CIP-002-4 and recommends a "yes" vote despite imperfections with the language of draft Appendix A. SME recommends comments in the hope that the language yet will be clarified. Specifically, Seattle City Light commends the change to a "bright-line" approach to identifying Critical Assets as proposed in draft CIP-002-4. The use of nationwide criteria reasonably captures as Critical Assets the large generating units and high voltage transmission facilities essential to the reliable operation of the North American Bulk Power System. The flexibility afforded individual Planning Coordinators and Transmission Planners to specify additional facilities as Critical Assets important to local reliability furthers the objective of Bulk Power System reliability by allowing some smaller generating units and transmission facilities to be called out as Critical Assets without drawing in all assets of a certain size that are not critical elsewhere. These changes are consistent with Seattle City Light's philosophy towards Critical Assets, which always has been about stepping up and acknowledging the importance of identifying and protecting all Critical Assets essential to the reliability of the bulk power system. Ultimately CIP-002-4 as proposed promises to benefit the electricity industry, consumers, and North America by improving reliability through a certain and consistent application of the Critical Asset identification process. That said, Seattle City Light SME expresses concern that imperfections in the language of draft CIP-002-4 may frustrate its promise of bringing Critical Asset certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust among industry, regulators, government, and the public at large. As such the comments below are offered as potential corrections to the details of draft and not as reflecting on the "bright-line" approach of proposed CIP-002-4. 1. Requirement 2 of draft CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable

Voter	Entity	Segment	Vote	Comment
				operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Seattle City Light is finding the term 'shared Cyber Assets' unclear and suggests clarification as follows: "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." 2. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV of higher with three or more other transmission stations." Seattle City Light agrees with Lower Colorado River Authority that additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator-does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 3. Critical Asset criterion 1.13 indicates that "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes" are Critical Assets. Seattle City Light concurs with the assessment of APPA and others that this wording may inadvertently include any SCADA system that controls 300 MW or more of load (and thus has 'capability' to shed it), and recommends wording similar to item 1.11 of draft CIP-010-1, "BES elements that perform automatic aggregate load shedding of 300 MW or more within 15 minutes."

Response: Thank you for your comments.

1) Requirement R2 has been changed to clarify the issues presented.
2) Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion.
3) Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."

Voter	Entity	Segment	Vote	Comment
Allen Klassen	Westar Energy	1	Affirmative	Westar shares and would echo many of the concerns already expressed by other entities, but is casting an affirmative vote to move this process forward.
Response: Thank you for your comments.				
Peter T Yost	Consolidated Edison Co. of New York	3	Affirmative	1. New Requirement R1: We request an explicit definition of "annual." In addition, it is not clear whether the "update as necessary" applies to updates to the list during the annual review. The language should be clarified to more definitely express the "update as necessary" to be applicable to the list during the annual review. 2. New Requirement R2: In addition, there is no reason for the parenthetical with the specific inclusion of nuclear generation. It should be removed. 3. Attachment 1/Requirement R2: We suggest the removal of "control system" and "backup control system" in Attachment 1, Part 1.14. These systems should be identified as part of new Requirement R2, Critical Cyber Asset Identification. 4. Attachment 1: Part 1.3 is extremely broad and is under defined. Either delete it or provide additional specificity delineating the limited range of circumstances when a PC or TP may designate a facility as critical. 5. Attachment 1: Part 1.10 uses the phrase "the loss of the assets" without describing the relevant time period. Are these assets losses for a few cycles, for a few minutes, for a few hours or for a few days? We recommend that the conclusion of Part 1.10 state "...would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3 for a period of xx hours (e.g., 24 hours) or more." 6. Implementation Plan: Agreed, so long as an Entity can have access to an exception process with an implementation plan to request additional time due to a large increase in identified assets, without a self-reported violation, within an implementation schedule.
Response: Thank you for your comments. 1) The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects to correct this phraseology in the next version. 2) The parenthetical statement about nuclear generation comes from Attachment 1 criterion 1.1. 3) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which				

Voter	Entity	Segment	Vote	Comment
				states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." 4) Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." 5) The phrase "loss of assets" is not limited to any period of time. A trip and a 24 hour outage would both apply. 6) Thank you for your comments.
Henry Ernst-Jr	Duke Energy Carolina	3	Affirmative	Duke Energy appreciates the drafting team's work, and offers the following comments, which are also being submitted via the comment form: 1. We agree that the revised CIP-002-4 will lead to an improvement in reliability. However, CIP-003 through CIP-009 need modifications other than just changing the revision numbers, as evidenced by numerous interpretation requests and general confusion in the industry. While we understand that the plan is to complete those modifications in 2011, industry will be adding numerous Critical Assets and Critical Cyber Assets due to these revisions to CIP-002. Applying the current versions of CIP-003 through CIP-009 to numerous additional Critical Cyber Assets compounds the difficulty of maintaining compliance without more clear direction. 2. CIP-002-4 Attachment 1 criteria need further clarification. a. 1.1 - Consistent with Criteria 1.8 and 1.9, this criterion should be conditioned by adding the phrase "unless planning studies are available to demonstrate that the loss of generation does not cause violation of one or more Interconnection Reliability Operating Limits (IROLs)." Related to the generation loss impact on Interconnection frequency and resource adequacy, Duke Energy disagrees with the arbitrary selection of the generation loss MW amount for the following reasons: o System inertia and frequency response factor into potential impact a generation loss could have on Interconnection frequency, and are different for each Interconnection. A 1,500 MW loss in the Eastern Interconnection is much less significant in terms of the initial frequency deviation than a similar loss within any other Interconnection. o The limit fails to recognize the options available to the Balancing Authority to restore its balance within the existing criteria of the NERC reliability standards. For example, recovery from the loss of 1,500 MW within a 5,000 MW Balancing Authority may be quite different than recovery from a 1,500 MW loss within a 135,000 MW Balancing Authority in the Eastern Interconnection. PJM alone is about

Voter	Entity	Segment	Vote	Comment
				twice the size of ERCOT. b. 1.2 - We believe that 1000 MVAR may too large, and should be reduced to 500 MVAR. However criterion 1.2 could just be deleted, since any significant reactive resources would be picked up under criterion 1.8 c. 1.3 - "Generation designated as required for reliability purposes" doesn't seem to be a very "bright-line". We believe this criterion should be further clarified by including language from the "Rationale and Implementation Reference Document". d. 1.4 - Need to clarify that this criterion only includes the primary Blackstart Resources. Entities may include various alternative resources in their restoration plans which aren't Critical Assets, but which may not be clearly distinguished from the primary Blackstart Resources in the restoration plan. Add the phrase "that the entity intends to rely on for system restoration". e. 1.5 - The CIPDT is looking to the industry to define Critical Assets based on NERC definitions that are somewhat ambiguous and can be redefined by Standard Drafting Teams any time a group of standards is proposed. This could lead to Critical Assets being removed or added without proper analysis being performed on the impact to the system. Also, the definition of Cranking Path could be debated that it could be from a generating source that provides electricity to a larger resource during restoration. This source could be a small diesel that is sitting next to a large generator that provides the electricity to lift pumps, exciter field, or some other device that provides the means for a larger generator to become a Blackstart Resource. Or it could be argued that the cranking path is from a Blackstart Resource to fossil plants on the system that are used to facilitate the restoration of the system. Duke Energy requests that the Drafting team rewrite this requirement so that it does not use this term. Duke Energy also believes that the CIPDT should get input from those that are familiar with Restoration by requesting input from the Emergency Operations Drafting Team. We propose rewriting 1.5 as follows: The Facilities comprising the current carrying path from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point where multiple path options exist. f. 1.8 & 1.9 - These two criteria need clarification. First, it should be made clear that this IROL evaluation is to be made in the planning timeframe, because the purpose is to identify Critical Cyber Assets that need to be protected, which is an activity that takes place in the planning timeframe. Also, including the word "destroyed" in the phrase "destroyed, degraded,

Voter	Entity	Segment	Vote	Comment
				misused or otherwise rendered unavailable" creates significant uncertainty regarding what the IROL analysis is intended to encompass. Add the phrase "via cyber attack" after the word "unavailable". This will clarify that the evaluation only encompasses destruction, degradation or misuse that can be achieved via cyber attack, and not a physical attack on the station. For example, physical attack could imply multiple transmission lines shorted to ground, which entails a much different analysis than transmission lines removed from service via cyber attack. NOTE: The physical security provided by the CIP standards is focused on protection of the Critical Cyber Assets, not the Critical Assets. g. 1.10 - As with our comment on 1.8 & 1.9 above, add the phrase "via cyber attack" after the word "unavailable". We also have a concern that if an entity fails to identify a facility under 1.1 or 1.3, they will also be in violation for failing to identify the corresponding Transmission Facilities under 1.10 (i.e. the double jeopardy issue). Need to replace the phrase "described in" with the phrase "identified by an entity pursuant to". Alternatively, 1.10 could be folded into 1.1 and 1.3 by adding the phrase "and Transmission Facilities providing the generation interconnection" to those criteria. h. 1.11 - Need to clarify that these Transmission Facilities are those that are specifically identified in the Nuclear Plant Interface Requirements (NPIRs) in the Agreement developed between the Nuclear Plant Generator Operator and applicable Transmission Entities pursuant to NUC-001-2. At the end of this criterion add the phrase "in the Agreement(s) required by NUC-001 R2." i. 1.12 - As with our comment on 1.8 & 1.9 above, this criterion should be revised to clarify that this IROL evaluation is to be made in the planning timeframe, because the purpose is to identify Critical Cyber Assets that need to be protected, which is an activity that takes place in the planning timeframe. Also, the phrase "destroyed, degraded, misused or otherwise rendered unavailable" needs to be clarified by adding the phrase "via cyber attack" after the word "unavailable". j. 1.13 - Load control programs shouldn't be defined as Critical Assets but rather Critical Cyber Assets, since they are a function of the control center, which is already a Critical Asset. Replace the word "Common" with the phrase "Each control center or backup control center used to". Also, clarify the meaning of "automatic" by inserting the parenthetical (without human intervention) after the word "automatic". k. 1.14 - This criterion is far too broad because we don't have an approved

Voter	Entity	Segment	Vote	Comment
				NERC definition of control room, control system, backup control room or backup control system. Many switchyards and substations have control systems that could be used to perform transmission functions, but that doesn't mean that they are "Critical Assets". Remove control system and backup control system from this criterion and limit it to identifying the control centers and backup control centers associated with the Critical Assets on the transmission system, just as criteria 1.15 links identification of the control center or backup co

Response: Thank you for your comments.

The SDT agrees that other changes ultimately need to be made to the body of CIP standards, and expects to post them next year.

Item 1.1 - Prior drafts had wording about reserve sharing for the threshold. The SDT received feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily. The drafting team conducted an informal survey of the regions, and identified what the megawatt value of the reserve sharing would be for various groups. The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions. Based on information provided on the DOE website, the SDT believes that an increased amount of generation capacity will be classified as Critical Assets in the US.

Item 1.2 – The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.4 – A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." EOP-005-2 R1.4 states that the restoration plan must include "Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit." The SDT feels that these Blackstart Resources must be classified as Critical Assets. It should be noted that not all blackstart generators must be designated as Blackstart Resources.

Item 1.5 – NERC standard EOP-005-2 R1.5, "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started," designates that Cranking Paths must be identified.

Items 1.8 & 1.9 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets.

Item 1.10 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets. There is no double jeopardy, since all

Voter	Entity	Segment	Vote	Comment
of these criteria are contained in the same Requirement. Item 1.11 – The SDT does not believe that adding the phrase "in the Agreement(s) required by NUC-001 R2" provides any clarification, since the defined NERC term Nuclear Plant Interface Requirements is "The requirements based on NPLRs and Bulk Electric System requirements that have been mutually agreed to by the Nuclear Plant Generator Operator and the applicable Transmission Entities." Item 1.12 – Cyber analysis is contained in Requirement R2, not in the identification of Critical Assets. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Kevin Querry	FirstEnergy Solutions	3	Affirmative	FirstEnergy appreciates the CIP Standard Drafting Team's (SDT) careful consideration of our and other stakeholder feedback during prior comment periods and the SDT's decision to develop the CIP-002-4 bright-line standard. The development of CIP-002-4 and continued use of the CIP-003 through CIP-009 standards brings needed industry consistency in Critical Asset determinations while appropriately building upon prior industry efforts of implementing the CIP standards. FirstEnergy supports CIP-002-4 and is voting AFFIRMATIVE for the standard but believes changes are needed to better clarify Attachment 1. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. Lastly, we encourage the SDT to reconsider its Implementation Plan for the CIP version 4 standards. The Implementation Plan is a 15 page document which is overly complex and difficult to understand. Please refer to FE's comments submitted through the parallel comment period for suggestions for improvement and simplification. The following are FirstEnergy's proposed Attachment 1 changes: 1) Criterion 1.8 currently states "Transmission Facilities at a single station

Voter	Entity	Segment	Vote	Comment
				location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).” Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014. C.) A possible misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say “Transmission Facilities at a single station location ...” not all transmission facilities at a single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8: “1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL).” The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states “Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements” Clarity needed: The term “essential” is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the following change for 1.11: “1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements.” 3) Criterion 1.5 currently states “The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.” FirstEnergy suggests replacing the word “multiple” with “two or more” for clarity. 4) Criterion 1.14 currently states “Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.” FirstEnergy suggests removing the

Voter	Entity	Segment	Vote	Comment
				text "control system" and "or backup control system" for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the "control center" then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase "control system" is vague.

Response: Thank you for your comments.

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.

R Scott S. Barfield-McGinnis	Georgia System Operations Corporation	3	Affirmative	Additional clarity is needed to criteria 1.15 in Attachment 1 regarding what constitutes control. For example, merely sending set points to a generator which will reject those inputs if they are outside preset parameters should not constitute control of that generation.

Response: Thank you for your comments.

Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection."

Voter	Entity	Segment	Vote	Comment
Charles Locke	Kansas City Power & Light Co.	3	Affirmative	The bright lines established by the proposed standard have not been established with a strong engineering basis and do not necessarily reflect a true measure of reliability impact to the bulk electric system. It is recommended to develop a process to determine a true reliability assessment and adjust the bright line proposed here to a deliberate and supportable definition.
Response: Thank you for your comments. Please refer to the response to comments document.				
David Burke	Orange and Rockland Utilities, Inc.	3	Affirmative	1. New Requirement R1: ORU requests an explicit definition of "annual." In addition, it is not clear whether the "update as necessary" applies to updates to the list during the annual review. The language should be clarified to more definitely express the "update as necessary" to be applicable to the list during the annual review. 2. New Requirement R2: In addition, there is no reason for the parenthetical with the specific inclusion of nuclear generation. It should be removed. 3. Attachment 1/Requirement R2: ORU suggests the removal of "control system" and "backup control system" in Attachment 1, Part 1.14. These systems should be identified as part of new Requirement R2, Critical Cyber Asset Identification. 4. Attachment 1: Part 1.3 is extremely broad and is under defined. Either delete it or provide additional specificity delineating the limited range of circumstances when a PC or TP may designate a facility as critical. 5. Attachment 1: Part 1.10 uses the phrase "the loss of the assets" without describing the relevant time period. Are these assets losses for a few cycles, for a few minutes, for a few hours or for a few days? We recommend that the conclusion of Part 1.10 state "...would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3 for a period of xx hours (e.g., 24 hours) or more." 6. Implementation Plan: Agreed, so long as an Entity can have access to an exception process with an implementation plan to request additional time due to a large increase in identified assets, without a self-reported violation, within an implementation schedule.
Response: Thank you for your comments. 1) The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects to correct this phraseology in the next version.				

Voter	Entity	Segment	Vote	Comment
2) The parenthetical statement about nuclear generation comes from Attachment 1 criterion 1.1. 3) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." 4) Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." 5) The phrase "loss of assets" is not limited to any period of time. A trip and a 24-hour outage would both apply. 6) Thank you for your comments.				
Dana Wheelock	Seattle City Light	3	Affirmative	Specifically, Seattle City Light commends the change to a "bright line" approach to identifying Critical Assets as proposed in draft CIP-002-4. The use of nationwide criteria reasonably captures as Critical Assets the large generating units and high voltage transmission facilities essential to the reliable operation of the North American Bulk Power System. The flexibility afforded individual Planning Coordinators and Transmission Planners to specify additional facilities as Critical Assets important to local reliability furthers the objective of Bulk Power System reliability by allowing some smaller generating units and transmission facilities to be called out as Critical Assets without drawing in all assets of a certain size that are not critical elsewhere. These changes are consistent with Seattle City Light's philosophy towards Critical Assets, which always has been about stepping up and acknowledging the importance of identifying and protecting all Critical Assets essential to the reliability of the bulk power system. Ultimately CIP-002-4 as proposed promises to benefit the electricity industry, consumers, and North America by improving reliability through a certain and consistent application of the Critical Asset identification process. That said, Seattle City Light expresses concern that imperfections in the language of draft CIP-002-4 may frustrate its promise of bringing Critical Asset certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust

Voter	Entity	Segment	Vote	Comment
				among industry, regulators, government, and the public at large. As such the comments below are offered as potential corrections to the details of draft and not as reflecting on the "bright-line" approach of proposed CIP-002-4. 1. Requirement 2 of draft CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Seattle City Light follows Tacoma Power in finding the term 'shared Cyber Assets' unclear and suggests clarification as follows: "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." 2. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV of higher with three or more other transmission stations." Seattle City Light agrees with Lower Colorado River Authority that additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator-does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 3. Critical Asset criterion 1.13 indicates that "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes" are Critical Assets. Seattle City Light concurs with the assessment of APPA and others that this wording may inadvertently include any SCADA system that controls 300 MW or more of load (and thus has 'capability' to shed it), and recommends wording similar to item 1.11 of draft CIP-010-1, "BES elements that perform automatic aggregate load shedding of 300 MW or more within 15 minutes." 4. Critical Asset criterion 1.15 states "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Seattle City Light concurs with APPA in understanding that this criterion is intended to apply to control centers controlling multiple

Voter	Entity	Segment	Vote	Comment
				units, and recommends the following wording: "Each control center or backup control center used to control multiple generation units identified as Critical Assets, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection."
Response: Thank you for your comments. 1) Requirement R2 has been changed to clarify the issues presented. 2) Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Assets Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion. 3) Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." 4) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Travis Metcalfe	Tacoma Public Utilities	3	Affirmative	Tacoma Power has submitted comments during the comment period for Version 4 of the CIP standards. If there is a subsequent future ballot for Project 2008-06, consideration of all submitted comments need to be reflected in such ballot.
Response: Thank you for your comments. Please refer to the response to comments document.				
Guy Andrews	Georgia System Operations Corporation	4	Affirmative	Additional clarity is needed to criteria 1.15 in Attachment 1 regarding what constitutes control. For example, merely sending set points to a generator which will reject those inputs if they are outside preset parameters should not constitute control of that generation.
Response: Thank you for your comments. Item 1.15 –This criterion has been changed to "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control				

Voter	Entity	Segment	Vote	Comment
center used to control aggregate generation equal to or exceeding 1500 MWs in a single Interconnection."				
Douglas Hohlbaugh	Ohio Edison Company	4	Affirmative	FirstEnergy appreciates the CIP Standard Drafting Team's (SDT) careful consideration of our and other stakeholder feedback during prior comment periods and the SDT's decision to develop the CIP-002-4 bright-line standard. The development of CIP-002-4 and continued use of the CIP-003 through CIP-009 standards brings needed industry consistency in Critical Asset determinations while appropriately building upon prior industry efforts of implementing the CIP standards. FirstEnergy supports CIP-002-4 and is voting AFFIRMATIVE for the standard but believes changes are needed to better clarify Attachment 1. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. Lastly, we encourage the SDT to reconsider its Implementation Plan for the CIP version 4 standards. The Implementation Plan is a 15 page document which is overly complex and difficult to understand. Please refer to FE's comments submitted through the parallel comment period for suggestions for improvement and simplification. The following are FirstEnergy's proposed Attachment 1 changes: 1) Criterion 1.8 currently states "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014. C.) A possible misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say "Transmission Facilities at a single station location ..." not all transmission facilities at a single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8: "1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL)." The Planning

Voter	Entity	Segment	Vote	Comment
				Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements" Clarity needed: The term "essential" is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the following change for 1.11: "1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements." 3) Criterion 1.5 currently states "The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist." FirstEnergy suggests replacing the word "multiple" with "two or more" for clarity. 4) Criterion 1.14 currently states "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." FirstEnergy suggests removing the text "control system" and "or backup control system" for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the "control center" then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase "control system" is vague.

Response: Thank you for your comments.

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2, "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Voter	Entity	Segment	Vote	Comment
Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.				
Hao Li	Seattle City Light	4	Affirmative	Specifically, Seattle City Light commends the change to a "bright-line" approach to identifying Critical Assets as proposed in draft CIP-002-4. The use of nationwide criteria reasonably captures as Critical Assets the large generating units and high voltage transmission facilities essential to the reliable operation of the North American Bulk Power System. The flexibility afforded individual Planning Coordinators and Transmission Planners to specify additional facilities as Critical Assets important to local reliability furthers the objective of Bulk Power System reliability by allowing some smaller generating units and transmission facilities to be called out as Critical Assets without drawing in all assets of a certain size that are not critical elsewhere. These changes are consistent with Seattle City Light's philosophy towards Critical Assets, which always has been about stepping up and acknowledging the importance of identifying and protecting all Critical Assets essential to the reliability of the bulk power system. Ultimately CIP-002-4 as proposed promises to benefit the electricity industry, consumers, and North America by improving reliability through a certain and consistent application of the Critical Asset identification process. That said, Seattle City Light expresses concern that imperfections in the language of draft CIP-002-4 may frustrate its promise of bringing Critical Asset certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust among industry, regulators, government, and the public at large. As such

Voter	Entity	Segment	Vote	Comment
				the comments below are offered as potential corrections to the details of draft and not as reflecting on the "bright-line" approach of proposed CIP-002-4. 1. Requirement 2 of draft CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Seattle City Light follows Tacoma Power in finding the term 'shared Cyber Assets' unclear and suggests clarification as follows: "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." 2. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV of higher with three or more other transmission stations." Seattle City Light agrees with Lower Colorado River Authority that additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator-does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 3. Critical Asset criterion 1.13 indicates that "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes" are Critical Assets. Seattle City Light concurs with the assessment of APPA and others that this wording may inadvertently include any SCADA system that controls 300 MW or more of load (and thus has 'capability' to shed it), and recommends wording similar to item 1.11 of draft CIP-010-1, "BES elements that perform automatic aggregate load shedding of 300 MW or more within 15 minutes." 4. Critical Asset criterion 1.15 states "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Seattle City Light concurs with APPA in understanding that this criterion is intended to apply to control centers controlling multiple units, and recommends the following wording: "Each control center or

Voter	Entity	Segment	Vote	Comment
				backup control center used to control multiple generation units identified as Critical Assets, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection."
Response: Thank you for your comments. 1) Requirement R2 has been changed to clarify the issues presented. 2) Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion. 3) Item 1.13 – This criterion has been changed to "System(s) or facilities that perform automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." 4) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Keith Morisette	Tacoma Public Utilities	4	Affirmative	Tacoma Power has submitted comments during the comment period for Version 4 of the CIP standards. If there is a subsequent future ballot for Project 2008-06, consideration of all submitted comments need to be reflected in such ballot.
Response: Thank you for your comments. Please refer to the response to comments document.				
Max Emrick	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	5	Affirmative	Tacoma Power has submitted comments during the comment period for Version 4 of the CIP standards. If there is a subsequent future ballot for Project 2008-06, consideration of all submitted comments need to be reflected in such ballot.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Please refer to the response to comments document.				
Amir Y Hammad	Constellation Power Source Generation, Inc.	5	Affirmative	This affirmative ballot is contingent on successfully addressing specific comments submitted on the Formal Comment Form for Project 2008-06 Cyber Security 706.
Response: Thank you for your comments. Please refer to the response to comments document.				
Kenneth Dresner	FirstEnergy Solutions	5	Affirmative	FirstEnergy appreciates the CIP Standard Drafting Team's (SDT) careful consideration of our and other stakeholder feedback during prior comment periods and the SDT's decision to develop the CIP-002-4 bright-line standard. The development of CIP-002-4 and continued use of the CIP-003 through CIP-009 standards brings needed industry consistency in Critical Asset determinations while appropriately building upon prior industry efforts of implementing the CIP standards. FirstEnergy supports CIP-002-4 and is voting AFFIRMATIVE for the standard but believes changes are needed to better clarify Attachment 1. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. Lastly, we encourage the SDT to reconsider its Implementation Plan for the CIP version 4 standards. The Implementation Plan is a 15 page document which is overly complex and difficult to understand. Please refer to FE's comments submitted through the parallel comment period for suggestions for improvement and simplification. The following are FirstEnergy's proposed Attachment 1 changes: 1) Criterion 1.8 currently states "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014. C.) A possible

Voter	Entity	Segment	Vote	Comment
				misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say “Transmission Facilities at a single station location ...” not all transmission facilities at a single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8: “1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL).” The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states “Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements” Clarity needed: The term “essential” is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the following change for 1.11: “1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements.” 3) Criterion 1.5 currently states “The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.” FirstEnergy suggests replacing the word “multiple” with “two or more” for clarity. 4) Criterion 1.14 currently states “Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.” FirstEnergy suggests removing the text “control system” and “or backup control system” for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the “control center” then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase “control system” is vague.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval.				
Michelle DAntuono	Occidental Chemical	5	Affirmative	Although Occidental Chemical has voted to approve CIP-002-4, we are concerned about the ambiguous wording under Criterion 1.3 "Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes." Although clarified in the CIP-002-4 Rationale and Implementation Reference Document as those generation facilities designated as "Reliability Must Run", the language in the standard is the ultimate arbiter. We understand that not all regions use the term "Reliability Must Run", but Criterion 1.3 as written is too open-ended - which violates the intent of NERC's goal to develop requirements that are clear and measurable.
Response: Thank you for your comments. Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."				

Voter	Entity	Segment	Vote	Comment
Annette M Bannon	PPL Generation LLC	5	Affirmative	Regarding Attachment 1, section 1.1, a generation plant that is tripped as part of a Remedial Action Scheme (Special Protection System) to protect the Bulk Electric System should be exempted from Critical Asset designation. The inclusion of a generation plant in a RAS scheme infers that the plant is not critical to the operation of the BES. NERC included this same criteria in their guidance document "Security Guideline for the Electricity Sector: Identifying Critical Assets," page 10, table C-2.
Response: Thank you for your comments. The Remedial Action Scheme would be covered under criterion 1.12. The plant would not be exempted if it met any of the criteria in Attachment 1.				
Michael J. Haynes	Seattle City Light	5	Affirmative	Specifically, Seattle City Light commends the change to a "bright-line" approach to identifying Critical Assets as proposed in draft CIP-002-4. The use of nationwide criteria reasonably captures as Critical Assets the large generating units and high voltage transmission facilities essential to the reliable operation of the North American Bulk Power System. The flexibility afforded individual Planning Coordinators and Transmission Planners to specify additional facilities as Critical Assets important to local reliability furthers the objective of Bulk Power System reliability by allowing some smaller generating units and transmission facilities to be called out as Critical Assets without drawing in all assets of a certain size that are not critical elsewhere. These changes are consistent with Seattle City Light's philosophy towards Critical Assets, which always has been about stepping up and acknowledging the importance of identifying and protecting all Critical Assets essential to the reliability of the bulk power system. Ultimately CIP-002-4 as proposed promises to benefit the electricity industry, consumers, and North America by improving reliability through a certain and consistent application of the Critical Asset identification process. That said, Seattle City Light SME expresses concern that imperfections in the language of draft CIP-002-4 may frustrate its promise of bringing Critical Asset certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust among industry, regulators, government, and the public at large. As such the comments below are offered as potential corrections to the details of draft and not as reflecting on the "bright-line" approach of proposed CIP-002-4.

Voter	Entity	Segment	Vote	Comment
				1. Requirement 2 of draft CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Seattle City Light follows Tacoma Power in finding the term 'shared Cyber Assets' unclear and suggests clarification as follows: "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." 2. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV of higher with three or more other transmission stations." Seattle City Light agrees with Lower Colorado River Authority that additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator-does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 3. Critical Asset criterion 1.13 indicates that "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes" are Critical Assets. Seattle City Light concurs with the assessment of APPA and others that this wording may inadvertently include any SCADA system that controls 300 MW or more of load (and thus has 'capability' to shed it), and recommends wording similar to item 1.11 of draft CIP-010-1, "BES elements that perform automatic aggregate load shedding of 300 MW or more within 15 minutes." 4. Critical Asset criterion 1.15 states "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Seattle City Light concurs with APPA in understanding that this criterion is intended to apply to control centers controlling multiple units, and recommends the following wording: "Each control center or backup control center used to control multiple generation units identified as Critical Assets, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection."

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. 1) Requirement R2 has been changed to clarify the issues presented. 2) Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion. 3) Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." 4) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Scott M. Helyer	Tenaska, Inc.	5	Affirmative	Regarding the Critical Asset Criteria, it seems that the 300 MW referred to in 1.13 should be 1500 MW to make it consistent with generation.
Response: Thank you for your comment. Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program."				
Martin Bauer P.E.	U.S. Bureau of Reclamation	5	Affirmative	The vote reflects that project can generally move forward we offer the following comments to improve the criterion in CIP-002-4 Attachment 1. Criterion 1.1 uses the phrase "aggregate highest rated net Real Power capability. The Rationale and Implementation Reference Document states the term "net Real Power capability" is drawn from MOD-024. However, use of that standard is questionable on at least two counts, the first being that it has yet to be approved by FERC, and that it is a "fill-in-the-black" standard that FERC has stated it finds unacceptable. As MOD-024 would rely on the Reliability Assurer's procedures, it could not assure a uniform application across the Interconnections. We suggest instead "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest Facility Rating, pursuant to FAC-008/009, equal

Voter	Entity	Segment	Vote	Comment
				to or exceeding 1500 MW." Criterion 1.8 refers to conditions which would "violate one or more Interconnection Reliability Operating Limits (IROLs)" for transmission Facilities at a single station. However, Transmission Owners are not on the list of Responsible Entities with whom coordination of identified SOL's or IROL's is required in the Reliability Standards. This would make it difficult for a Transmission Owner to assess the facility based on the criterion. Criterion 1.12 has similar requirements as Criterion 1.8, but applies to Special Protection Systems, Remedial Action Schemes or automated switching systems. Where a Responsible Entity either provides information to one of these systems/schemes or responds to such a scheme, without being the "owner/operator" of the scheme may not be privy to knowing if an IROL is or could be violated. This would make it difficult for the Responsible Entity to assess the facility based on the criterion. We suggest that a requirement that Responsible Entities, who have the Reliability Standards obligations to identify System Operating Limits (SOL's) and IROL's, must respond if requested by a Responsible Entity whom they are not currently required notify. This would permit the Responsible Entity to assess his facility or systems/schemes.
Response: Thank you for your comments. Item 1.1 – The SDT chose to use "net Real Power capability" instead of Facility Rating due to the fact that it is a more accurate reflection on generation output to the system. Items 1.8 and 1.12 – FAC-014-2 R5 states "The Reliability Coordinator, Planning Authority and Transmission Planner shall each provide its SOLs and IROLs to those entities that have a reliability-related need for those limits and provide a written request that includes a schedule for delivery of those limits as follows:"				
Nickesha P Carrol	Consolidated Edison Co. of New York	6	Affirmative	1. New Requirement R1: We request an explicit definition of "annual." In addition, it is not clear whether the "update as necessary" applies to updates to the list during the annual review. The language should be clarified to more definitely express the "update as necessary" to be applicable to the list during the annual review. 2. New Requirement R2: In addition, there is no reason for the parenthetical with the specific inclusion of nuclear generation. It should be removed. 3. Attachment 1/Requirement R2: We suggest the removal of "control system" and "backup control system" in Attachment 1, Part 1.14. These systems should be identified as part of new Requirement R2, Critical Cyber Asset Identification.

Voter	Entity	Segment	Vote	Comment
				4. Attachment 1: Part 1.3 is extremely broad and is under defined. Either delete it or provide additional specificity delineating the limited range of circumstances when a PC or TP may designate a facility as critical. 5. Attachment 1: Part 1.10 uses the phrase "the loss of the assets" without describing the relevant time period. Are these assets losses for a few cycles, for a few minutes, for a few hours or for a few days? We recommend that the conclusion of Part 1.10 state "…would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3 for a period of xx hours (e.g., 24 hours) or more." 6. Implementation Plan: Agreed, so long as an Entity can have access to an exception process with an implementation plan to request additional time due to a large increase in identified assets, without a self-reported violation, within an implementation schedule.
Response: Thank you for your comments. 1) The phraseology you are concerned about exists in the existing CIP-002-3 standard. The SDT expects to correct this phraseology in the next version. 2) The parenthetical statement about nuclear generation comes from Attachment 1 criterion 1.1. 3) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." 4) Item 1.3 – This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." 5) The phrase "loss of assets" is not limited to any period of time. A trip and a 24-hour outage would both apply. 6) Thank you for your comments.				
Mark S Travaglianti	FirstEnergy Solutions	6	Affirmative	FirstEnergy appreciates the CIP Standard Drafting Team's (SDT) careful consideration of our and other stakeholder feedback during prior comment periods and the SDT's decision to develop the CIP-002-4 bright-line standard. The development of CIP-002-4 and continued use of the CIP-003 through CIP-009 standards brings needed industry consistency in Critical Asset determinations while appropriately building upon prior industry efforts of implementing the CIP standards. FirstEnergy supports CIP-002-4

Voter	Entity	Segment	Vote	Comment
				and is voting AFFIRMATIVE for the standard but believes changes are needed to better clarify Attachment 1. In our view, some of the criteria are vaguely written and subject to interpretation - specifically criteria 1.8 and 1.11 - and we offer suggestions for improving expectations and compliance certainty. Additionally, we suggest less substantive changes to criteria 1.5 and 1.14 for clarity and consistency. Lastly, we encourage the SDT to reconsider its Implementation Plan for the CIP version 4 standards. The Implementation Plan is a 15 page document which is overly complex and difficult to understand. Please refer to FE's comments submitted through the parallel comment period for suggestions for improvement and simplification. The following are FirstEnergy's proposed Attachment 1 changes: 1) Criterion 1.8 currently states "Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)." Clarity needed: A.) It is not evident who is responsible for identifying the applicable transmission facilities covered by 1.8. B.) Item 1.8 should rely on review/analysis that is regularly performed by industry in meeting other NERC reliability standards. Item 1.8 should be based on IROL determinations made from planning horizon studies and information communicated to responsible entities via FAC-010/FAC-014. C.) A possible misinterpretation of Attachment 1, Item 1.8 is that it is intended to review a complete loss of substation. However the words say "Transmission Facilities at a single station location ..." not all transmission facilities at a single substation location. Based on the above items, FirstEnergy proposes the following for item 1.8: "1.8. Transmission Facilities designated by the Planning Coordinator or Transmission Planner that, if destroyed, degraded, misused or otherwise rendered unavailable, demonstrates the need for an Interconnection Reliability Operating Limit (IROL)." The Planning Coordinator and Transmission Planner determine and communicate IROLs in the planning time horizon per NERC reliability standard FAC-014. The subject Transmission Facilities are the contingency Transmission Facilities communicated by the PC and TP per requirement R5 of FAC-014. The 1.8 criterion should not appear to require any new study or analysis by the TP or PC. 2) Criterion 1.11 currently states "Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements" Clarity needed: The term "essential" is vague and open to interpretation. FE suggests that the SDT focus on Transmission Facilities identified in Nuclear Plant Interface Requirements identified as providing offsite power supply for nuclear plant safety requirements. We propose the

Voter	Entity	Segment	Vote	Comment
				following change for 1.11: "1.11 Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements." 3) Criterion 1.5 currently states "The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist." FirstEnergy suggests replacing the word "multiple" with "two or more" for clarity. 4) Criterion 1.14 currently states "Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator." FirstEnergy suggests removing the text "control system" and "or backup control system" for consistency to criteria 1.15. If the intent is to ensure coverage of offsite data centers or telecommunication centers that support the "control center" then the SDT should provide a separate criterion in Attachment 1. To extend coverage of 1.14 and not 1.15 is inconsistent and the use of the phrase "control system" is vague.

Response: Thank you for your comments.

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements.

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."

The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters

Voter	Entity	Segment	Vote	Comment
after regulatory approval.				
Silvia P Mitchell	Florida Power & Light Co.	6	Affirmative	The standard CIP-002-4 includes a more consistent method for the evaluation of Critical Assets and removes the variability that is introduced when letting Entity's perform their own risk-based methodology. It is requested to include an exception process in the implementation plan for a company that has a large number of new CA(s). For consistency, make all of the cases fall under the 24 month timeline to remove the possible misinterpretation of the Categories as stated in proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities. The only exception to the 24-month requirement shall be those newly identified CCAs and Responsible Entities that require compliance before commissioning. Depending on the number of CCAs a utility needs to protect, the resources needed to accomplish the lockdowns may not be available. We recommend a 24-month implementation time frame for all categories. This would make the criteria for compliance more consistent. Industry will be competing for cyber security resources for implementation. We are also very concerned that the expectation is to replace CCA's with TFEs with assets not requiring an exception. In general, this is the correct direction to go in, but in practice this is not necessarily easy. For example, If tomorrow an asset with a TFE fails in service and needs to be replaced with a similar asset, it instead must be replaced with a "technically compliant" asset. This may be impractical early on as stocking levels may be inadequate and qualified replacements may not have been fully vetted for the application.
Response: Thank you for your comments. Thank you for your comments. The SDT has simplified the Implementation Plan to reference the Effective Date of CIP-002-4 through CIP-009-4 which is 8 calendar quarters after regulatory approval				
Jessica L Klinghoffer	Kansas City Power & Light Co.	6	Affirmative	The bright-lines established by the proposed standard have not been established with a strong engineering basis and do not necessarily reflect a true measure of reliability impact to the bulk electric system. It is recommended to develop a process to determine a true reliability assessment and adjust the bright-line proposed here to a deliberate and supportable definition.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comment. The SDT believes that the implementation of Attachment 1 criteria will increase the consistency of Critical Asset identification over the existing entity defined risk-based methodology.				
Dennis Sismaet	Seattle City Light	6	Affirmative	Seattle City Light Subject Matter Expert (SME) supports the changes proposed for CIP-002-4 and recommends a "yes" vote despite imperfections with the language of draft Appendix A. SME recommends comments in the hope that the language yet will be clarified. Specifically, Seattle City Light commends the change to a "bright-line" approach to identifying Critical Assets as proposed in draft CIP-002-4. The use of nationwide criteria reasonably captures as Critical Assets the large generating units and high voltage transmission facilities essential to the reliable operation of the North American Bulk Power System. The flexibility afforded individual Planning Coordinators and Transmission Planners to specify additional facilities as Critical Assets important to local reliability furthers the objective of Bulk Power System reliability by allowing some smaller generating units and transmission facilities to be called out as Critical Assets without drawing in all assets of a certain size that are not critical elsewhere. These changes are consistent with Seattle City Light's philosophy towards Critical Assets, which always has been about stepping up and acknowledging the importance of identifying and protecting all Critical Assets essential to the reliability of the bulk power system. Ultimately CIP-002-4 as proposed promises to benefit the electricity industry, consumers, and North America by improving reliability through a certain and consistent application of the Critical Asset identification process. That said, Seattle City Light SME expresses concern that imperfections in the language of draft CIP-002-4 may frustrate its promise of bringing Critical Asset certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust among industry, regulators, government, and the public at large. As such the comments below are offered as potential corrections to the details of draft and not as reflecting on the "bright-line" approach of proposed CIP-002-4. 1. Requirement 2 of draft CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable

Voter	Entity	Segment	Vote	Comment
				operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." Seattle City Light follows Tacoma Power in finding the term 'shared Cyber Assets' unclear and suggests clarification as follows: "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those Cyber Assets networked to a system that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." 2. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV of higher with three or more other transmission stations." Seattle City Light agrees with Lower Colorado River Authority that additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator-does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 3. Critical Asset criterion 1.13 indicates that "Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes" are Critical Assets. Seattle City Light concurs with the assessment of APPA and others that this wording may inadvertently include any SCADA system that controls 300 MW or more of load (and thus has 'capability' to shed it), and recommends wording similar to item 1.11 of draft CIP-010-1, "BES elements that perform automatic aggregate load shedding of 300 MW or more within 15 minutes." 4. Critical Asset criterion 1.15 states "Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection." Seattle City Light concurs with APPA in understanding that this criterion is intended to apply to control centers controlling multiple units, and recommends the following wording: "Each control center or backup control center used to control multiple generation units identified as Critical Assets, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection."
Response: Thank you for your comments. 1) Requirement R2 has been changed to clarify the issues presented. 2) Item 1.7 – The intent of Criterion 1.7 is to classify as a Critical Asset a Transmission Facility operated at 300 kV or higher at stations				

Voter	Entity	Segment	Vote	Comment
interconnected at 300 kV or higher with three or more other transmission stations. That includes upstream, downstream, networked, and radial. It should be noted that connections to generators or generation only substations are not counted in this Criterion. The source to the radial substation may be considered a Critical Asset, but the radial substation would not be considered a Critical Asset since by definition it cannot be connected to three or more transmission substations. There is no distance requirement in the criterion. 3) Item 1.13 – This criterion has been changed to "Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." 4) Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection."				
Michael C Hill	Tacoma Public Utilities	6	Affirmative	Tacoma Power has submitted comments during the comment period for Version 4 of the CIP standards. If there is a subsequent future ballot for Project 2008-06, consideration of all submitted comments need to be reflected in such ballot.
Response: Thank you for your comments. Please refer to the response to comments document.				
Brian Evans-Mongeon	Utility Services, Inc.	8	Affirmative	Utility Services endorses the comments as submitted by the NPCC Regional Standards Committee, as well as the American Public Power Association (APPA). We thank the SDT for their continued efforts to address this difficult matter and urge them to consider the comments from both of these organizations as a means to strengthen the standard and its requirements.
Response: Thank you for your comments. Please refer to the response to comments document.				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	Removal of the Canadian Nuclear exclusion is problematic for many of NPCC's Canadian members. Although the drafting team believed that in all cases the Canadian Nuclear Safety Commission would have authority, the onice to demonstrate and prove that the standard wouldn't apply to Canadian nukes is a burden in the view of some.

Voter	Entity	Segment	Vote	Comment
Response: Thank you for your comments. The SDT is aware that the removal of the nuclear plant exclusion in response to a FERC order brought Canadian nuclear plants into the CIP standards. That was unintentional and will be corrected in the revised standards next posted for ballot.				
David Batz	Edison Electric Institute	1	Abstain	EEI believes that the adoption of a uniform and consistent methodology for the selection of Critical Assets will enhance the reliability of the bulk power system. EEI offers the following suggested revisions for Attachment 1: ..... 1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW. 1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater. 1.3. Each generation Facility that the Planning Coordinator or Transmission Planner has designated as required to avoid one or more reliability criteria violations. 1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan. 1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where two or more path options exist. 1.6. Transmission Facilities operated at 500 kV or higher. 1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations. 1.8. Transmission Facilities at a single station location that the Planning Coordinator or Transmission Planner has designated that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROL) violations. 1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, would result in one or more Interconnection Reliability Operating Limit (IROLs) violations. 1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.

Voter	Entity	Segment	Vote	Comment
				1.11. Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements. 1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROLs) violations for failure to operate as designed. 1.13.Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes. 1.14. Each control center, , or backup control center, used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. 1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection. 1.16. Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include.

Response: Thank you for your comments.

Item 1.1 – The guidance document posted by the SDT provides direction on the location issue. "Single plant location" refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

Item 1.3 –This criterion has been reworded to "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon."

Item 1.5 – This criterion has been reworded to "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist as identified in the Transmission Operator's restoration plan."

Item 1.8 – This criterion has been changed to "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Item 1.9 – This criterion has been changed to "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."

Voter	Entity	Segment	Vote	Comment
Item 1.11 – Criterion 1.11 is based on NUC-001-2 R9.2.2, "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." It is not limited to offsite power requirements. Item 1.12 – This criterion has been changed to "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limit (IROL) violations for failure to operate as designed." Item 1.14 – Based on industry comments received, criterion 1.14 has been reworded to "Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator." A new criterion, 1.16, has been added which states, "Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." A new criterion, 1.17, has also been added which states, "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection." Item 1.16 – In order to eliminate any confusion, the SDT has chosen to eliminate this criterion in the next ballot.				
Gary Ofner	North Carolina Electric Membership Corp.	1	Abstain	Although NCEMC supports replacing a subjective "Risk Based Methodology" with a "Bright-line Criteria" to identify critical assets, we believe many of the proposed criteria have not been technically justified on the basis that the proposed criteria properly identify those assets which could have a material impact on the reliability of the BES. If the proposed criteria are not modified to better reflect the impact of the assets on the reliability of the BES, then there should be a provision in the standard that provides a process for an entity to technically demonstrate that even though the criteria identifies some of their assets as Critical Assets, their assets (or a portion thereof) do not meet the definition of a Critical Asset and should be excluded from applicability of CIP-003 through CIP-009.
Response: Thank you for your comments. Please refer to the response to comments document. In addition, the SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.				
Gregory Van Pelt	California ISO	2	Abstain	The standard as written is flawed in that Applicability for this standard should be clearly stated to only include owners of the facilities or assets involved (i.e., "Critical Assets"). For example, broad sweeping designation of Transmission Operators or Balancing Authorities, as "Responsible Entities" is inappropriate in cases where they do not own the "Critical Assets". This creates undue and duplicative burden without benefit. Requirements should be revised to note a Responsible Entity is only a Responsible Entity for assets that it owns. The standard is an improvement

Voter	Entity	Segment	Vote	Comment
				in that clear criteria for designation of "Critical Asssets" is beneficial to consistent application and enforcement.
Response: Thank you for your comments. The Applicability section of the standard specifies to which NERC Registered Entities the standard applies. All Requirements apply to all Entities listed in the Applicability section. Each requirement uses the phrase "its ... Assets" to designate ownership.				
Barry Lawson	National Rural Electric Cooperative Association	4	Abstain	Please see NRECA submitted comments for reasons for abstaining during this ballot. If hte standard is modified as requested in our comments, we can vote in the affirmative.
Response: Thank you for your comments. Please refer to the response to comments document.				
Joanna Luong-Tran	TransAlta Centralia Generation, LLC	5	Abstain	TransAlta sumbitted comments to explain our abstain.
Response: Thank you for your comments. Please refer to the response to comments document.				

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4

Please **DO NOT** use this form to submit comments. Please use the electronic form located at the link below to submit comments on the proposed CIP Version 4 Standards and Implementation Plans. Comments must be submitted by **December 10, 2010.** If you have questions please contact Howard Gugel at howard.gugel@nerc.net or by telephone at (609) 651-2269.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Background:
In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) inter-dependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-002-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order 706 directives. CIP-010 and CIP-011were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT limited the scope of modifications to requirements in CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in FERC Order 706, paragraph 236. The approach to address the remaining FERC Order 706 directives continues to be developed.

The SDT believes the NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

The draft standard *CIP 002-4 – Cyber Security – Critical Cyber Asset Identification* identifies BES Cyber Systems according to "bright-line" criteria associated with the impact on reliable operation of the BES. The "bright-line" criteria is contained in *Attachment 1 – Critical Asset Criteria* of CIP-002-4.The *CIP-002-4 Cyber Security - Critical Asset Identification - Rationale and Implementation Reference Document* provides clarifying notes and rationale of the SDT. The draft CIP-003-4 through CIP-009-4 standards include conforming changes to match the versioning of CIP-002-4.

On September 20, 2010, the SDT posted CIP-002-4 for a formal 45-day comment period. During the comment period, the team received 101 sets of comments, including comments from more than 200 different people from approximately 125 companies representing 9 of the 10 Industry Segments. Concurrent with the comment period, a ballot pool was assembled and the first formal ballot was conducted. For the ballot a quorum was achieved, and the weighted sector vote was 43.33% affirmative.

Based on the comments received, a few changes were made to CIP-002-4.

- The Applicability section was modified to include an exemption for nuclear facilities regulated by the Canadian Nuclear Safety Commission, and Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.
- In addition, the effective date was changes to eight quarters after regulatory approval, so that entities are not required to maintain two sets of approved Critical Asset lists and Critical Cyber Asset lists during the implementation plan.
- Requirements R1 and R2 were modified slightly to clarify that each list must be updated on an ongoing basis, but the review and approval need only occur annually. Conforming changes were made to the compliance section.
- Finally, significant changes were made to Attachment 1 to ten of the criteria. One criterion was deleted, which allowed entities to place items on the Critical Asset list at their discretion.
    - The criterion for control centers was split into three criteria to allow for differentiation in size for Balancing Authorities and Transmission Operators.

All of these changes were in response to comments received.

A separate ballot is being conducted for CIP-005-4, and if the proposed standard is approved it will be filed with CIP-003-4 to CIP-009-4. If the proposed CIP-005-4 is rejected, then the present CIP-005-3 will be modified with conforming changes and filed with CIP-003-4 to CIP-009-4. The team is continuing to work on subsequent cyber security standards that will establish impact levels and define associated cyber security controls at levels appropriate to their BES impact.

The Team is seeking industry feedback on this draft of CIP 002-4. The industry feedback will be considered by the SDT in determining if there is a need to make any additional changes to CIP 002-4 requirements and related documents.

The SDT has provided a form for industry participants to offer their comments on this draft of CIP-002-4.

Question

Your response to the following question will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above.

1. When reviewing the changes to the proposed CIP-002-4 standard, do you believe that the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets?

   ☐ Yes

   ☐ No

   Comments:

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

NERC Cyber Security Standards Drafting Team for Order 706
September 2010

This document provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

TABLE OF CONTENTS

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION 3

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT 3

EXECUTIVE SUMMARY 3

INTRODUCTION 5

OVERALL APPLICATION OF ATTACHMENT 1 6

GENERATION 7

TRANSMISSION 11

CONTROL CENTERS 14

GUIDANCE ON THE IMPLEMENTATION PLAN 16

CONCLUSION 17

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

EXECUTIVE SUMMARY

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards and the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical

Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had

already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B, in the United States. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

OVERALL APPLICATION OF ATTACHMENT 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

GENERATION

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. This criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system.

  In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES. In a generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This may be illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility: in this case, the compromise of the cyber asset may result in an inability

of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant time before this affects real-time operation, time during which detection and remediation may be able to be effected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are designated as Critical Assets. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that

have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where two or more path options exist as Critical Assets. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where two or more paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time they are required or if they operate outside of the parameters they were designed for. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets.

- Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets, or used to control generation greater than an aggregate of 1500 MW in a single Interconnection, as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation

control center may cross multiple BA or RSG areas or even regions and Interconnections, and that BES impact will more likely be restricted within an Interconnection.

This criterion uses the phrase "control generation." Entities should consider the discussion of "control" for generation as discussed in the Frequently Asked Questions (FAQ) document for CIP 002-1, Question 9:

> **"Question:** *Are Cyber Assets for a control center or generation control center with monitoring only and no direct remote control required to be protected and secured under the Cyber Security Standards?*
> **Answer:** A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.
> An example of monitoring without direct control that is subject to the Cyber Security Standards is a Reliability Authority that receives data from Critical Cyber Assets to a state estimator. "

It must be noted that this part does not apply to those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document "Security Guideline for the Electric Sector: Identifying Critical Assets".

TRANSMISSION

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies, Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV

backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started". Part 1.5 specifies that the Facilities meeting these requirements or comprising the Cranking Paths be identified as Critical Assets.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

---

levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES: at this lower end of the EHV spectrum, the drafting team:
    - Excluded radial facilities that would only provide support for single generation facilities.
    - Specified interconnection to at least 3 transmission stations or substations to ensure that the level of impact would be appropriate.

- Parts 1.8 and 1.9 include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits,** R5.1.1 and R5.1.3.

- Part 1.10 designates those Transmission Facilities as Critical Assets that provide the generation interconnection for Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In

particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates as Critical Assets those systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Critical Assets.

  300 MW is the reporting threshold for DOE EIA-417.

CONTROL CENTERS

Parts 1.14 through 1.17 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation). While it is clear that the primary and all backup control centers operated by RCs, BAs, or TOPs **that meet the criteria** must be designated as Critical Assets, control centers at other applicable Responsible Entities that are used, by delegation, to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include

Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. It should be noted that Cyber Assets essential to the operation of a control center may be located at a data center that is not co-located with the control center itself.

- Part 1.14 designates all control centers used to perform the functional obligations of the Reliability Coordinator (RC) as Critical Assets. Each Reliability Coordinator control center and backup control center was included as a Critical Asset due to their key role in maintaining reliability for the Interconnection as a whole in concert with other Reliability Coordinators.

- For part 1.15, please refer to the discussion of generation control centers in the Generation section of this document.

- Part 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12. Due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. It must be noted that in many cases, some Transmission Operator functions are delegated to Transmission Owner control centers: in such cases, these must also be designated as Critical Assets. As with the discussion of part 1.15, the drafting team intended for the word control to have the same meaning as that found in *Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1* which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction."

- Part 1.17 specifies that all control centers that perform the functional obligations of a Balancing Authority (BA) that include at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13 must be declared as Critical Assets. In addition, this criterion designates as a Critical Asset any BA control center that, in aggregate, performs the functional obligations of a BA for 1500 MWs or more in a single Interconnection. The threshold, 'controls generation of 1500 MW' was chosen to maintain consistency with the threshold in part 1.1.

GUIDANCE ON THE IMPLEMENTATION PLAN

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. This implementation plan describes the schedule by which an Entity must become compliant with the Version 4 CIP Standards. Once this initial compliance milestone is reached, this implementation plan is effectively retired. For an Entity that registers after the Version 4 CIP Standards are effective or for those Critical Cyber Assets that are newly identify after the Version 4 CIP Standards are effective, Responsible Entities should refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* The *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* remains in use throughout the entire time that the Version 4 CIP Standards remain in effect.

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date[3] specified in the Standard or (ii) the compliance milestones in the version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This allows essentially a two year implementation period following FERC approval to become compliant with the Version 4 CIP Standards. Special consideration was given to maintain the compliance milestone date for those Critical Cyber Assets and Newly Registered Entities that are in the middle of their implementation period for the Version 3 Standards on the Effective Date of the Version 4 Standards.

The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one-time implementation window

[3] "The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)."

was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-002-4 through CIP-009-4.

Both the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* contain certain exceptions for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.

CONCLUSION

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

NERC Cyber Security Standards Drafting Team for Order 706
September 2010

This document ~~is intended to provide~~provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

TABLE OF CONTENTS

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION 3

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT 3

EXECUTIVE SUMMARY 3

INTRODUCTION 5

OVERALL APPLICATION OF ATTACHMENT 1 6

GENERATION 7

TRANSMISSION 11

CONTROL CENTERS 14

GUIDANCE ON THE IMPLEMENTATION PLAN 16

CONCLUSION 20

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

EXECUTIVE SUMMARY

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards and the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical

Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had

already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B~~.~~, in the United States. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

OVERALL APPLICATION OF ATTACHMENT 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it ~~is to leave~~leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity ~~should~~may choose to document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

GENERATION

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. This criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system.

- In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES. In a generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This may be illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility: in this case, the compromise of the cyber asset may result in an inability

of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant time before this affects real-time operation, time during which detection and remediation may be able to be effected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as ~~required~~necessary to ~~run to ensure reliable operation of~~avoid BES Adverse Reliability Impacts in the ~~BES~~ long term planning horizon are designated as Critical Assets. These Facilities ~~are often~~may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are ~~typically~~ designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these

Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where ~~multiple~~two or more path options exist as Critical Assets. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where ~~multiple~~two or more paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. ~~Since the purpose of~~ Special Protection Systems and Remedial Action Schemes ~~is~~may be implemented to prevent disturbances that would result in ~~excursions beyond~~exceeding IROLs~~, often in lieu of building additional Transmission Facilities,~~ if they do not provide the function required at the time ~~it is~~they are ~~expected that all such systems and schemes will be designated as Critical Assets.~~required or if ~~it~~they operates outside of the parameters ~~it was~~they were designed for. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets.

- Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets, or used to control generation greater than an aggregate of

1500 MW in a single Interconnection, as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections~~.~~ , and that BES impact will more likely be restricted within an Interconnection.

This criterion uses the phrase "control generation." Entities should consider the discussion of "control" for generation as discussed in the Frequently Asked Questions (FAQ) document for CIP 002-1, Question 9:

> **"Question:** *Are Cyber Assets for a control center or generation control center with monitoring only and no direct remote control required to be protected and secured under the Cyber ~~Cyber~~ Security Standards?*
> **Answer:** A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.
> An example of monitoring without direct control that is subject to the Cyber Security Standards is a Reliability Authority that receives data from Critical Cyber Assets to a state estimator. "

It must be noted that this part does not ~~include the term "control systems" to avoid including~~apply to those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document "Security Guideline for the Electric Sector: Identifying Critical Assets".

TRANSMISSION

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those

transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started. ". Part 1.5 specifies that the Facilities meeting these requirements or comprising the Cranking Paths be identified as Critical Assets.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies, Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES: at this lower end of the EHV spectrum, the drafting team:
    - Excluded radial facilities that would only provide support for single generation facilities.
    - Specified interconnection to at least 3 transmission stations or substations to ensure that the level of impact would be appropriate.

- Parts 1.8 and 1.9 include those Transmission Facilities that ~~would violate~~have been identified as critical to the derivation of IROLs ~~if they were rendered unavailable or degraded. By definition, IROLs are those operating limits that, if exceeded, would have a Wide-Area reliability impact.~~and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits,** R5.1.1 and R5.1.3.

- Part 1.10 designates those Transmission Facilities as Critical Assets that ~~directly connect~~provide the generation interconnection for Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. ~~By IROL definition~~The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed. By the ~~-~~definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates ~~those control systems~~ as Critical Assets those systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. ~~These may~~In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. ~~Control Systems that provide a "one-button push" capability of shedding 300 MW or more would also qualify~~ It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Critical Assets.

  300 MW is the reporting threshold for DOE EIA-417.

CONTROL CENTERS

Parts 1.14 ~~and~~ through 1.~~15~~17 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation). ~~Part 1.15 has already been discussed in the Generation section.~~

~~Part 1.14 designates all control centers and control systems used to perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA) or Transmission Operator (TOP). EOP-008 requires that RCs, BAs and TOPs "ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable."~~ While it is clear that the primary and all backup control centers operated by RCs, BAs, ~~and~~or TOPs **that meet the criteria** must be designated as Critical Assets, control ~~systems~~centers at other applicable Responsible Entities that are used, by delegation, to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include ~~control systems at~~ Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. ~~Control systems were specifically called out separately from control centers to ensure that Entities fully evaluate those systems used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. These control systems~~ It should be noted that Cyber Assets essential to the operation of a control center may be located at a data center that is not co-located with the control center itself.

~~.~~

- Part 1.14 designates all control centers used to perform the functional obligations of the Reliability Coordinator (RC) as Critical Assets. Each Reliability Coordinator control center and backup control center was included as a Critical Asset due to their key role in maintaining reliability for the Interconnection as a whole in concert with other Reliability Coordinators.

- For part 1.15, please refer to the discussion of generation control centers in the Generation section of this document.

- Part 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12. Due to the direct impact

on the operation of identified Critical Assets, these Transmission control centers –must be designated as Critical Assets. It must be noted that in many cases, some Transmission Operator functions are delegated to Transmission Owner control centers: in such cases, these must also be designated as Critical Assets. As with the discussion of part 1.15, the drafting team intended for the word control to have the same meaning as that found in *Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1* which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction."

- Part 1.17 specifies that all control centers that perform the functional obligations of ~~the~~ a Balancing Authority (BA) that include at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13 must be declared as Critical Assets. In addition, this criterion designates as a Critical Asset any BA control center that, in aggregate, performs the functional obligations of a BA for 1500 MWs or more in a single Interconnection. The threshold, 'controls generation of 1500 MW' was chosen to maintain consistency with the threshold in part 1.1.

GUIDANCE ON THE IMPLEMENTATION PLAN

~~In general, Responsible Entities must:~~

~~(1) Comply with CIP-002-4 on the Effective Date~~[3]

~~(2) Comply with CIP-003-4 through CIP-009-4 on the Effective Date for previously identified CCAs and~~

~~(3) Comply with CIP-003-4 through CIP-009-4 18 months after the Effective Date for any new Critical Cyber Assets identified as a result of Attachment 1 Criteria~~

[3] ~~"The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)." For example, if FERC approves CIP-002-4 on March 31, 2011, then US entities must be able to demonstrate compliance by October 1, 2011.~~

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*~~,~~ and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. ~~Responsible Entities should then~~This implementation plan describes the schedule by which an Entity must become compliant with the Version 4 CIP Standards. Once this initial compliance milestone is reached, this implementation plan is effectively retired. For an Entity ~~who~~that registers after the Version 4 CIP Standards are effective or for those Critical Cyber Assets that are newly identify after the Version 4 CIP Standards are effective, Responsible Entities should refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* ~~if directed to in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4.* Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard. Compliance milestones for CIP-003-4 through CIP-009-4 is determined based on specific cases outlined in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4.* These cases include the following:~~ . The *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* remains in use throughout the entire time that the Version 4 CIP Standards remain in effect.

- ~~Critical Cyber Assets Already in Compliance with CIP-003-3 through CIP-009-3~~

  ~~Since only conforming changes to CIP-003-3 through CIP-009-3 were made and no changes were made to the existing requirement language itself, those Critical Cyber Assets already in compliance with CIP-003-3 through CIP-009-3 should be compliant with CIP-003-4 through CIP-009-4 on the Effective Date of the Version 4 Standard.~~

- ~~Critical Cyber Assets at Critical Assets Newly Identified by CIP-002-4~~

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date[4] specified in the Standard or (ii) the compliance milestones

[4] "The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)."

in the version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This allows essentially a two year implementation period following FERC approval to become compliant with the Version 4 CIP Standards. Special consideration was given to maintain the compliance milestone date for those Critical Cyber Assets and Newly Registered Entities that are in the middle of their implementation period for the Version 3 Standards on the Effective Date of the Version 4 Standards.

The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one-time implementation window was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-~~003-4 through CIP-009-4. Since updates to the Critical Asset list must be made as necessary and since these updates may occur before the next scheduled annual review of the Critical Asset list as defined in CIP-002-4 R1, this implementation window is defined as a rolling window for the first 12 month period following the effective date of CIP-002-4.~~ 002-4 through CIP-009-4.

> ~~This rolling implementation window is only applicable to those Entities that have already defined Critical~~ Both the *Implementation Plan for Version 4 of* Cyber ~~Assets according to previous versions of~~ *Security Standards* CIP-002~~. Since these Entities already have fully developed~~ *-4 through* CIP~~ programs, the implementation window for these newly identified Critical Cyber Assets is 18 months. This implementation window is shorter than the 24 month implementation period given to Entities that do not currently have existing Critical Cyber Assets as per~~ *-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*~~.~~

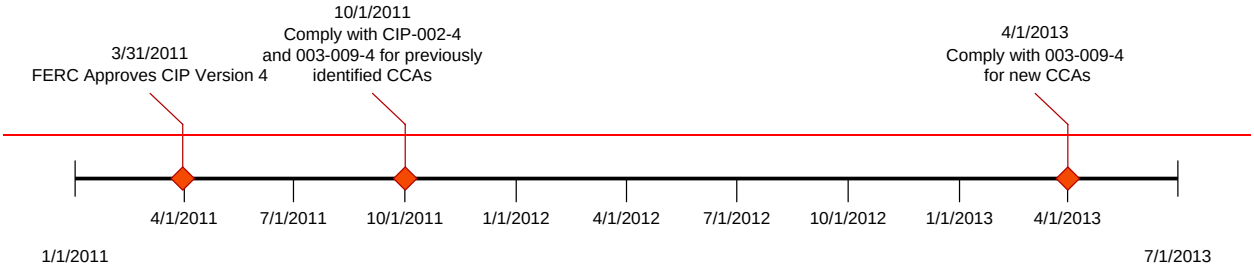
~~This special implementation window is slightly modified~~ contain certain exceptions for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.

- ~~All Other Critical Cyber Assets~~

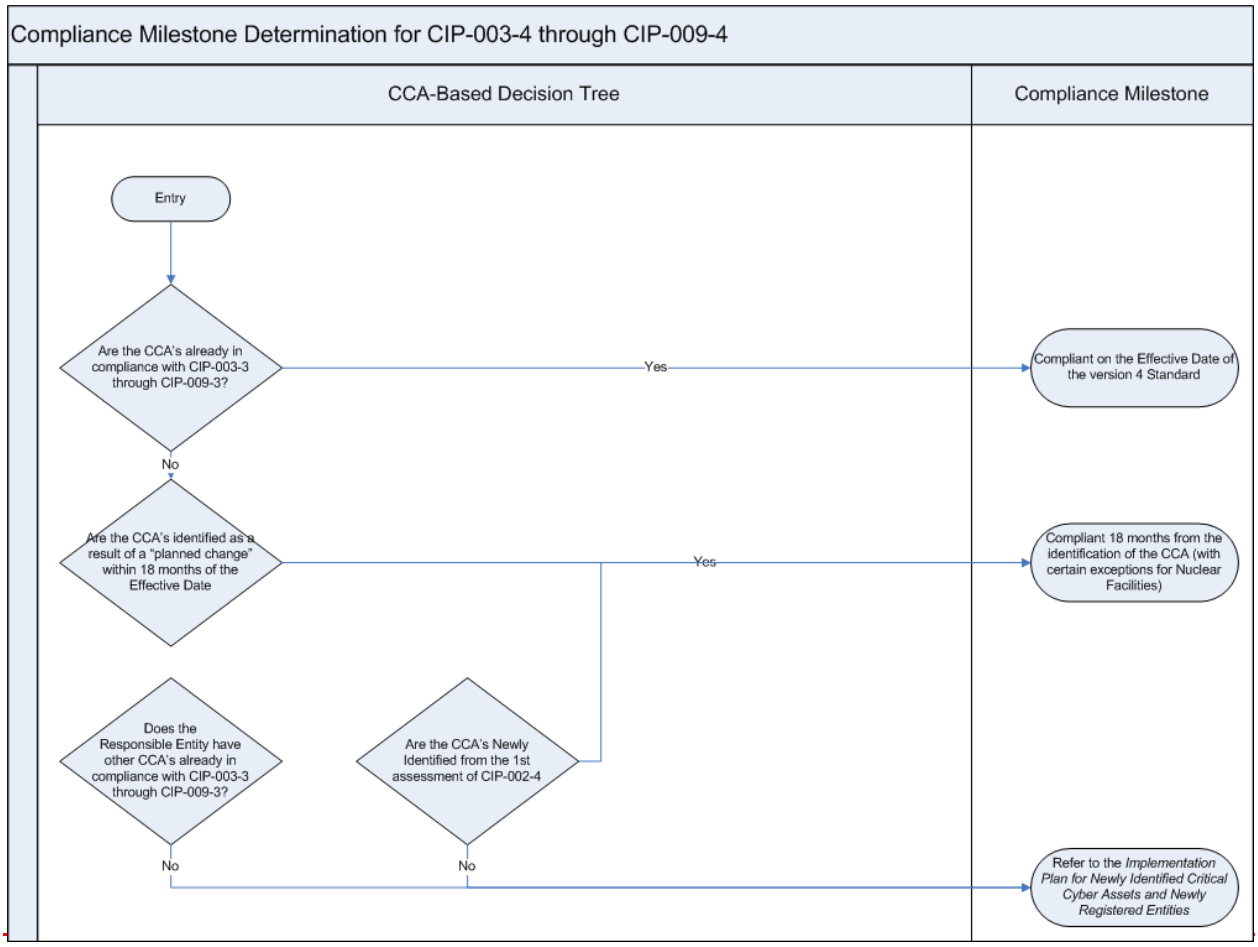
> ~~The compliance milestones for all other circumstances should be derived from the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered*~~

~~*Entities.* The modifications made to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* over the previous version of this plan were only those needed to conform to the Version 4 Standards.~~

~~The process for determining the compliance milestones for CIP-003-4 through CIP-009-4 is illustrated in the timeline and flowchart below.~~



~~**Figure 1: Sample Implementation Plan Timeline (General Case)**~~



CONCLUSION

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by*

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

the Responsible Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

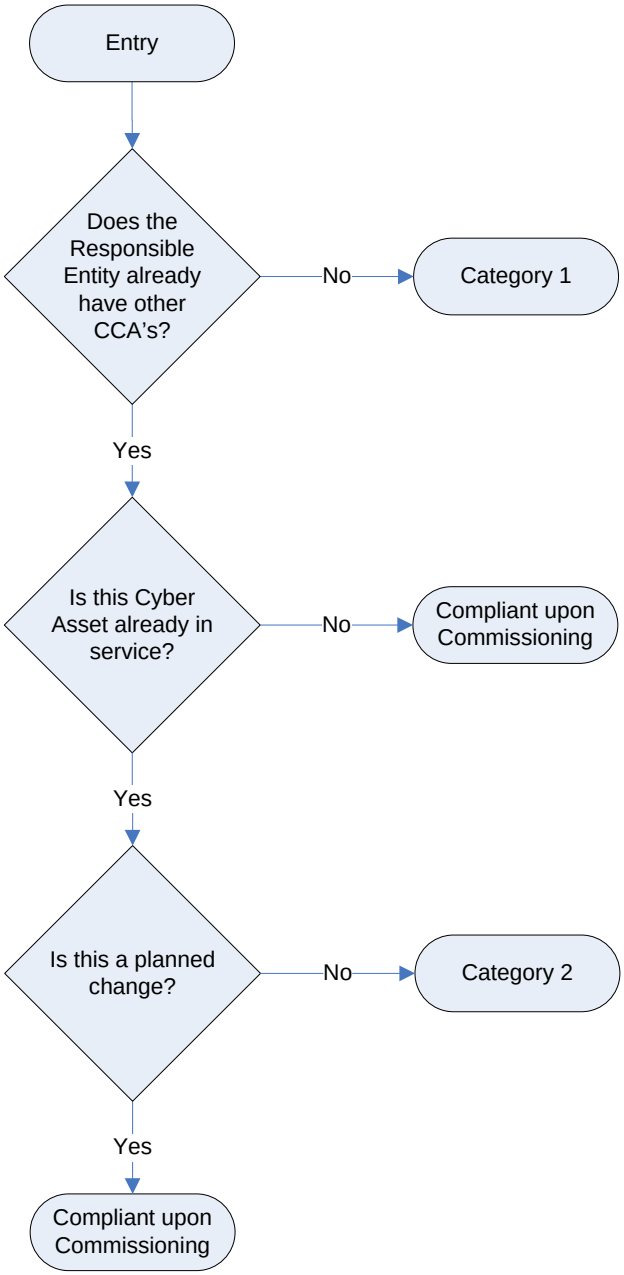


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In

this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the access authorization process.

The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merged plan is being performed. Progress towards meeting milestones and completing the merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly identified Critical Asset, but no newly identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon identification of a Critical Asset without associated Critical Cyber Assets. Only upon identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets[4]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

[4] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5][6] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	**Registration + 12 months**	**Registration + 24 months**
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.
[6] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

~~In all cases where a *Compliant* milestone is specified in Table 2 (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant'[4]) one year following the *Compliant* milestone listed in this Implementation Plan.~~

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

~~[4] The term 'Auditably Compliant' (AC) used in this Implementation Plan for newly identified Critical Cyber Assets and newly Registered Entities means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12 calendar months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" [see (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1]. Since in all cases, the 'Auditably Compliant' dates are one calendar year following the 'Compliant' (C) date, the Auditably Compliant dates are not specified in this plan. The terms 'Begin Work' (BW) and 'Substantially Compliant' (SC) used in the Version 1 Implementation Plan are no longer used, and therefore are not referenced in this Implementation Plan.~~

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by the ~~Responsibility~~Responsible Entity* (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the ~~Responsibility~~Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

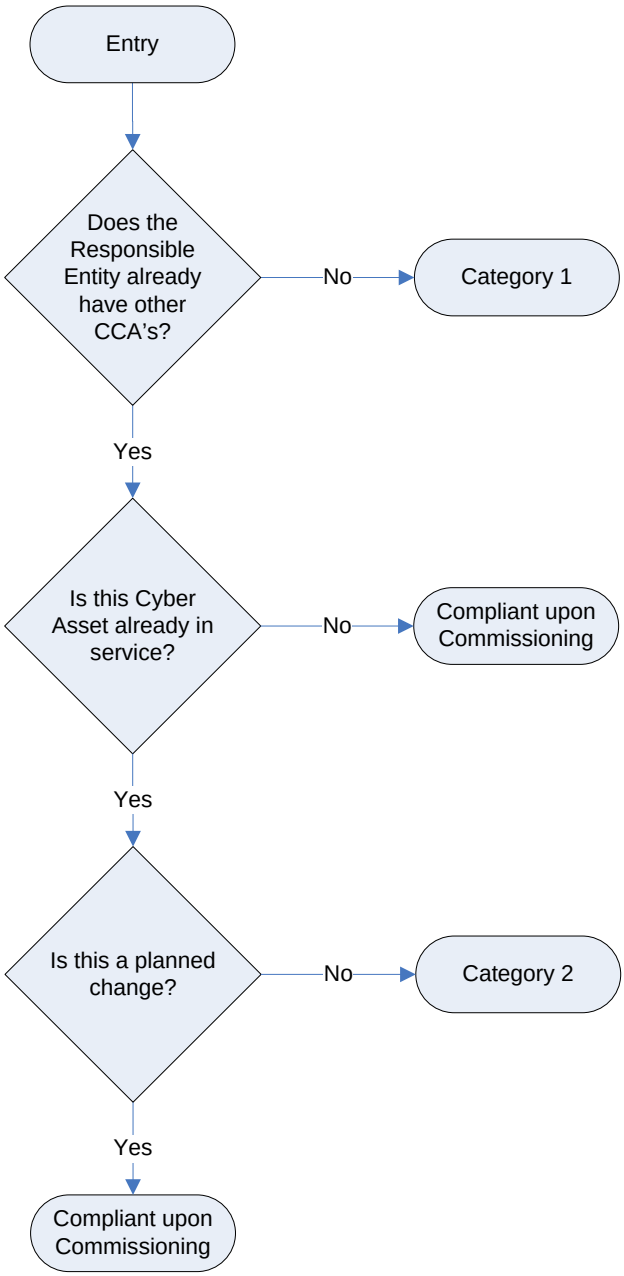


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   ~~The merged Registered Entity has one calendar year from the effective date of the business merger asset acquisition to continue to operate the separate Critical Asset identification processes while determining how to either combine the Critical Asset identification processes, or at a minimum, operate separate Critical Asset identifications under a common Senior Manager and governance structure. It would be preferred that a single program be the result, however, Registered Entity-specific circumstances may dictate or allow multiple programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.~~

   ~~The merged Registered Entity must ensure that it maintains the required 'annual application' of the Critical Asset identification as required in CIP-002 R1, even if that annual application timeframe is within the one calendar year allowed to determine if the merged Responsible Entity will combine the separate processes, or continue to operate them separately. Following the one calendar year allowance, the merged Responsible Entity must remain compliant with the program as it is determined to be implemented as a result of the one calendar year analysis of the disposition of the programs from the predecessor Responsible Entities.~~

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform

annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one ~~existing Critical Asset identification process and more than one~~ CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as ~~-~~'simple' as selection of different anti-virus tools, to something as ~~-~~'complicated' as the ~~Critical Asset identification. This scenario will be discussed in two sections, the first dealing with the combination of the Critical Asset identification methodologies; the second dealing with combining the CIP compliance implementation programs.~~access authorization process.

~~**(a) Combining the Critical Asset identification processes:** The merged Responsible Entity has one calendar year from the effective date of the business merger or asset acquisition to continue to operate the separate Critical Asset identification processes while~~

~~determining how to either combine the Critical Asset identification processes, or at a minimum, operate the separate Critical Asset identification processes under a common Senior Manager and governance structure. It would be preferred that a single program be the result, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002.~~

~~Registered Entities are encouraged when combining separate Critical Asset identification processes to ensure that, absent extraordinary circumstances, the resulting process produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entities' Critical Asset identification processes, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets. The combined Critical Asset identification and resultant Critical Asset list and Critical Cyber Asset list will be subject to review as part of compliance with NERC Reliability Standard CIP-002 R1 and R2. If additional Critical Assets are identified as a result of the application of the merged Critical Asset identification, they should be treated as newly identified Critical Cyber Assets, as discussed elsewhere in this Implementation Plan, and subject to the CIP compliance implementation program merger determination as discussed next.~~

~~Combining the CIP compliance implementation programs:~~

~~(b)~~ The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This '~~merge~~merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the ~~merge~~merged plan is being performed. Progress towards meeting milestones and completing the ~~merge~~merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly ~~designated~~identified Critical Asset, but no newly ~~designated~~identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon ~~designation~~identification of a Critical Asset without associated Critical Cyber Assets. Only upon ~~designation~~identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
~~Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology~~	~~Category 1~~	~~Category 2~~
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an~~-~~other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets[5]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
~~R4~~	~~*N/A*~~	~~*N/A*~~
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months

[5] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
R8	24 months	12 months
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[6][7] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	Registration + 12 months	Registration + 24 months
	~~All Facilities~~	~~All Facilities~~
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[6] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.

[7] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage,

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before these standards can be implemented.

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard, or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4; (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage; or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before ~~this~~ these standards can be implemented.

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 — Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

~~These standards are posted for ballot by NERC together with this Implementation Plan.~~ When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities
Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard, ~~.~~

~~**Proposed Effective Date for CIP-003-4 – CIP-009-4**~~
~~**Critical Cyber Assets Already in Compliance with CIP-003-3 – CIP-009-3**~~

~~Critical Cyber Assets identified by CIP-002-4 R2 that are already compliant with CIP-003-3 through CIP-009-3 shall be compliant with the requirements of CIP-003-4 through CIP-009-4 on~~ or (ii) the ~~Effective Date~~compliance milestones specified in ~~each~~ version ~~4 Standard.~~

~~**Critical Cyber Assets Associated with Critical Assets**~~ 3 of the *Implementation Plan for Newly Identified* ~~**by CIP-002-4**~~ *Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets ~~which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4~~ shall be compliant with CIP-~~003~~002-4 through CIP-009-4 by the ~~latter~~later of (i) ~~18 months after~~ the Effective Date ~~of~~in CIP-002-4 ~~or~~through CIP-009-4~~,~~; (ii) 6 months following the completion of the first refueling outage beyond ~~18 months from~~ the Effective Date of CIP-002-4 for those requirements requiring a refueling outage~~,~~; or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

~~*All Facilities Other Than U.S. Nuclear Power Plant Facilities*~~
~~For Responsible Entities who previously identified Critical Cyber Assets under CIP-002-1 R3, CIP-002-2 R3, or CIP-002-3 R3; Critical Cyber Assets associated with Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4.~~

~~**All Other Critical Cyber Assets**~~

~~For all cases not identified above, Critical Cyber Assets shall be compliant with the requirements of **CIP-003-4 through CIP-009-4** by the latter of (i) the Effective Date specified in each Version 4 Standard or (ii) the compliance milestones in the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* based on the earliest date of identification of the Critical Cyber Asset from CIP-002-1 R3, CIP-002-2 R3, CIP-002-3 R3, or CIP-002-4 R2.~~

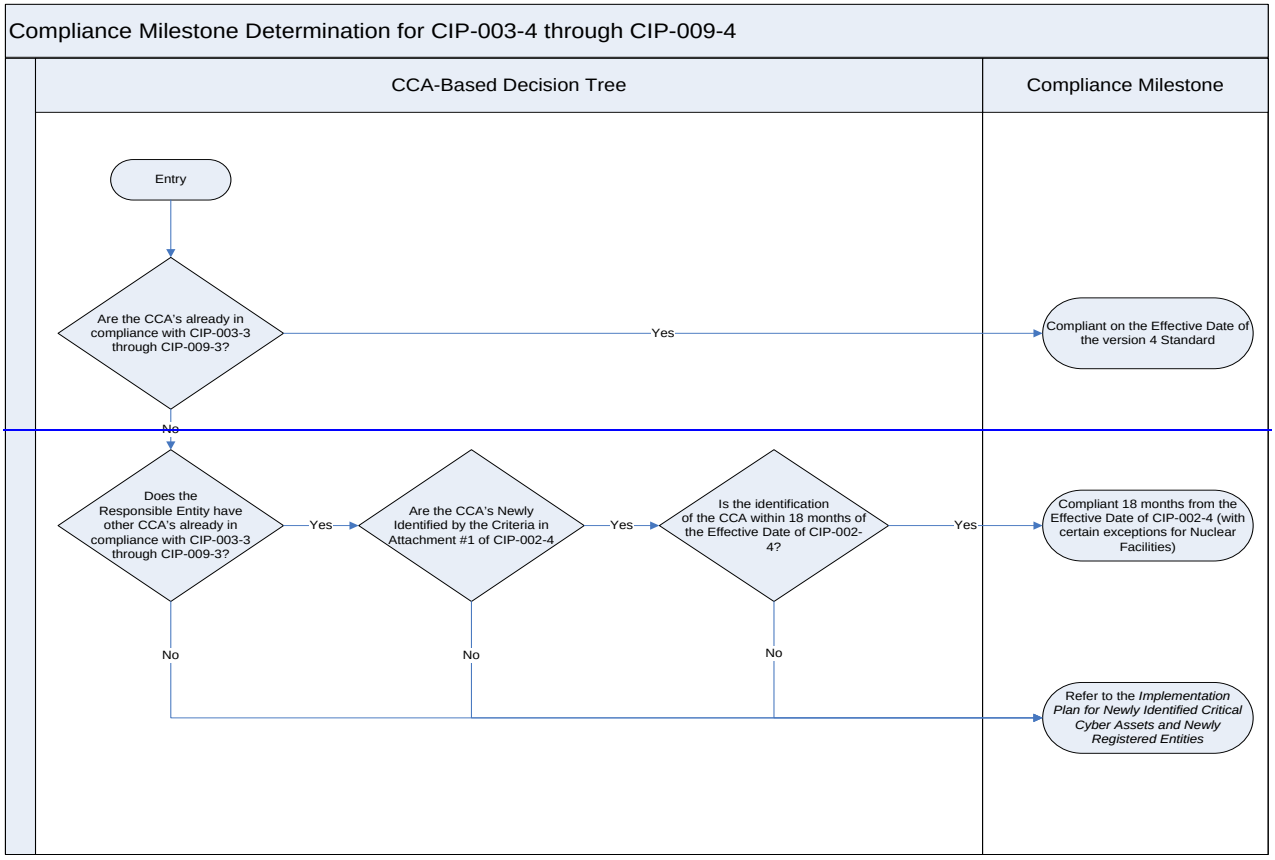
Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any ~~newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation Plan would apply based on the situations identified in the above section, *Proposed Effective Date*. This Implementation Plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to~~

~~annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.~~
Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

~~Prior Version Standard Retirement~~
~~Standards CIP-002-3 – CIP-009-3 shall be retired upon the Effective Date of the corresponding Version 4 Standard.~~


Compliance Milestone Determination for CIP-003-4 through CIP-009-4
CCA-Based Decision Tree
Compliance Milestone
Entry
Are the CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Compliant on the Effective Date of the version 4 Standard
No
Does the Responsible Entity have other CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Are the CCA's Newly Identified by the Criteria in Attachment #1 of CIP-002-4
Yes
Is the identification of the CCA within 18 months of the Effective Date of CIP-002-4?
Yes
Compliant 18 months from the Effective Date of CIP-002-4 (with certain exceptions for Nuclear Facilities)
No
No
No
Refer to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~3~~4

3. Purpose: NERC Standards CIP-002-~~3~~4 through CIP-009-~~3~~4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-~~3~~4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of ~~a risk-based assessment~~the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~**R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.~~

~~**R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.~~

~~**R1.2.** The risk-based assessment shall consider the following assets:~~

~~**R1.2.1.** Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.~~

~~**R1.2.2.** Transmission substations that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.3.** Generation resources that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.4.** Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.~~

~~**R1.2.5.** Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.~~

~~**R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.7.** Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.~~

~~**R2.**~~**R1.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the ~~risk-based assessment methodology required~~criteria contained in ~~R1.~~*CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary~~.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement ~~R2~~R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.~~ Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange.~~ The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary.~~ .

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

~~**R3.**~~ For the purpose of Standard CIP-002-~~3~~4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

~~**R3.1.**~~• The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

~~**R3.2.**~~• The Cyber Asset uses a routable protocol within a control center; or,

~~**R3.3.**~~• The Cyber Asset is dial-up accessible.

~~R4.~~R3. Annual Approval — The senior manager or delegate(s) shall approve annually the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1~~, R2,~~ and ~~R3~~R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

~~**M1.** The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.~~

~~M2.~~M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement ~~R2~~R1.

~~M3.~~M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement ~~R3~~R2.

~~M4.~~M3. The Responsible Entity shall make available its ~~approval~~ records of ~~annual~~ approvals as specified in Requirement ~~R4~~R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity~~ for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

~~R5.~~

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.1~~4.2.3 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.

5. Effective Date: The first day of the ~~third~~ eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update ~~review~~ this list as necessary~~at least annually~~, and ~~update~~ review it -at least annually~~as necessary~~.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. -The Responsible Entity shall update ~~review~~ this list as necessary~~at least annually~~, and ~~update~~ review it -at least annually~~as necessary~~.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that- could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1 ~~within 15 minutes~~. ~~The Responsible Entity shall review this list at least annually, and update it as necessary.~~

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- ~~**R1.1.**~~ The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- ~~**R1.2.**~~ The Cyber Asset uses a routable protocol within a control center; or,
- ~~**R1.3.**~~ The Cyber Asset is dial-up accessible.

~~**R2.**~~**R3.** Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of ~~the risk-based assessment methodology,~~ the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its ~~approval~~ records of ~~annual~~ approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

~~1.1.~~**1.2. The RE shall serve as the CEA with the following exceptions:**

~~1.1.1~~1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.~~Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.~~

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.~~ERO for Regional Entity.~~

~~1.1.2~~1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~1.1.3~~1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority~~Third-party monitor without vested interest in the outcome for NERC~~.

~~**1.2. Compliance Monitoring Period and Reset Time Frame**~~

~~Not applicable.~~

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment.	

		Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR~~s~~ or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon~~required for reliability purposes~~.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, ~~as identified in the Transmission Operator's restoration plan~~or up to the point on the Cranking Path where two or more~~multiple~~ path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of ~~, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of ~~, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to ~~directly~~ connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of ~~described in~~ Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause ~~violate~~ one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs ~~Common control system(s) capable of performing~~ automatic load shedding, without human operator initiation, of 300 MW or more

implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program~~within 15 minutes~~.

1.14. Each control center~~, control system,~~ or backup control center~~, or backup control system~~ used to perform the functional obligations of the Reliability Coordinator~~, Balancing Authority, or Transmission Operator~~.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4.~~identified as a Critical Asset,~~ Each control center or backup control center ~~or~~ used to control generation equal to or exceeding ~~greater than an aggregate of~~ 1500 MW~~s~~ in a single I~~i~~nterconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.~~Any additional assets that the Responsible Entity deems appropriate to include.~~

~~1.16.~~1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Successive Ballot Window Opens
Abbreviated Comment Period Opens
December 1-10, 2010

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Ballot Window December 1-10, 2010

A successive ballot will be conducted from 8:00 a.m. on Wednesday, December 1, 2010 through 8:00 p.m. on Friday, December 10, 2010. During the successive ballot window, members of the ballot pool associated with this project may log in and submit their votes from the following page:
https://standards.nerc.net/CurrentBallots.aspx

With a successive ballot, votes are **not** carried forward from the previous ballot. The Standards Committee encourages all members of the ballot pool to review the consideration of comments for the previous ballot and comment period and the modifications that team made to the standards and associated implementation plans.

Abbreviated Formal Comment Period Comment December 1-10, 2010

An abbreviated formal comment period will be open from December 1-10, 2010. The Standards Committee authorized the abbreviated comment period to support providing stakeholders with the opportunity to provide comment while also supporting the goal of completing this set of revisions before the end of December, 2010. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Project 2008-06 — Cyber Security 706

The drafting team working on "Version 4 CIP Standards" has posted its consideration of the comments submitted during the formal comment period and initial ballot that ended on November 3, 2010. Based on those comments, the drafting team modified CIP-002-4, the implementation plans, and the associated guidance document. Most revisions focused on 'fine tuning' the bright line criteria proposed for use in identifying critical assets. The proposed CIP-002-4 provides a significant improvement to CIP-002-3 by including a specific list of criteria for entities to use in identifying their critical assets.

Recognizing that protecting the cyber assets critical to the electric utility's infrastructure is also critical to national and international security, the revisions to CIP-002 are being advanced ahead of other improvements to the remaining set of CIP standards. The remaining CIP standards all rely on a complete and accurate identification of those assets that are critical to reliability. Because entities are so tightly interconnected, a vulnerability that seems insignificant to a single entity can place the entire grid in a state of vulnerability.

Each of the CIP standards (CIP-003-3 through CIP-009-3) contains at least one reference to CIP-002-3. To maintain clarity, CIP-003-3 through CIP-009-3 have had conforming changes made, so that all cross references within the set of standards are to "CIP Version 4" standards. *(CIP-005-4 - Cyber Security — Electronic Security Perimeter is posted separately, with a set of proposed revisions for expedited processing under Project 2010-15. If CIP-005-4 is not approved under Project 2010-15, it will be returned to this set of CIP standards.)*

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

Further details are available on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Successive Ballot Window Opens
Abbreviated Comment Period Opens
December 1-10, 2010

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Ballot Window December 1-10, 2010

A successive ballot will be conducted from 8:00 a.m. on Wednesday, December 1, 2010 through 8:00 p.m. on Friday, December 10, 2010. During the successive ballot window, members of the ballot pool associated with this project may log in and submit their votes from the following page:
https://standards.nerc.net/CurrentBallots.aspx

With a successive ballot, votes are **not** carried forward from the previous ballot. The Standards Committee encourages all members of the ballot pool to review the consideration of comments for the previous ballot and comment period and the modifications that team made to the standards and associated implementation plans.

Abbreviated Formal Comment Period Comment December 1-10, 2010

An abbreviated formal comment period will be open from December 1-10, 2010. The Standards Committee authorized the abbreviated comment period to support providing stakeholders with the opportunity to provide comment while also supporting the goal of completing this set of revisions before the end of December, 2010. Please use this electronic form to submit comments. If you experience any difficulties in using the electronic form, please contact Monica Benson at monica.benson@nerc.net. An off-line, unofficial copy of the comment form is posted on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Project 2008-06 — Cyber Security 706

The drafting team working on "Version 4 CIP Standards" has posted its consideration of the comments submitted during the formal comment period and initial ballot that ended on November 3, 2010. Based on those comments, the drafting team modified CIP-002-4, the implementation plans, and the associated guidance document. Most revisions focused on 'fine tuning' the bright line criteria proposed for use in identifying critical assets. The proposed CIP-002-4 provides a significant improvement to CIP-002-3 by including a specific list of criteria for entities to use in identifying their critical assets.

Recognizing that protecting the cyber assets critical to the electric utility's infrastructure is also critical to national and international security, the revisions to CIP-002 are being advanced ahead of other improvements to the remaining set of CIP standards. The remaining CIP standards all rely on a complete and accurate identification of those assets that are critical to reliability. Because entities are so tightly interconnected, a vulnerability that seems insignificant to a single entity can place the entire grid in a state of vulnerability.

Each of the CIP standards (CIP-003-3 through CIP-009-3) contains at least one reference to CIP-002-3. To maintain clarity, CIP-003-3 through CIP-009-3 have had conforming changes made, so that all cross references within the set of standards are to "CIP Version 4" standards. *(CIP-005-4 - Cyber Security — Electronic Security Perimeter is posted separately, with a set of proposed revisions for expedited processing under Project 2010-15. If CIP-005-4 is not approved under Project 2010-15, it will be returned to this set of CIP standards.)*

Next Steps

Voting results will be posted and announced after the ballot window closes.

Project Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

Further details are available on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_in
Ballot Period:	12/1/2010 - 12/10/2010
Ballot Type:	Initial
Total # Votes:	357
Total Ballot Pool:	410
Quorum:	**87.07 % The Quorum has been reached**
Weighted Segment Vote:	77.06 %
Ballot Results:	**The standard will proceed to recirculation ballot.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	113	1	82	0.788	22	0.212	3	6
2 - Segment 2.	11	0.8	3	0.3	5	0.5	3	0
3 - Segment 3.	93	1	64	0.865	10	0.135	5	14
4 - Segment 4.	30	1	19	0.792	5	0.208	4	2
5 - Segment 5.	87	1	52	0.8	13	0.2	6	16
6 - Segment 6.	51	1	30	0.789	8	0.211	4	9
7 - Segment 7.	1	0	0	0	0	0	0	1
8 - Segment 8.	10	0.6	3	0.3	3	0.3	0	4
9 - Segment 9.	5	0.4	4	0.4	0	0	0	1
10 - Segment 10.	9	0.9	9	0.9	0	0	0	0
Totals	**410**	**7.7**	**266**	**5.934**	**66**	**1.766**	**25**	**53**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	View
1	American Electric Power	Paul B. Johnson	Affirmative	View
1	American Transmission Company, LLC	Jason Shaver	Affirmative	View
1	Arizona Public Service Co.	Robert D Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	View

1	BC Transmission Corporation	Gordon Rawlings	Negative	View
1	Beaches Energy Services	Joseph S. Stonecipher	Negative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	View
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Brian Conroy		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Vero Beach	Randall McCamish	Affirmative	View
1	City Utilities of Springfield, Missouri	Jeff Knottek	Negative	View
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Abstain	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Commonwealth Edison Co.	Gregory Campbell		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	John K Loftis	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S.	Larry Monday		
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Abstain	View
1	Empire District Electric Co.	Ralph Frederick Meyer	Negative	View
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	GDS Associates, Inc.	Claudiu Cadar	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Robert Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	View
1	Keys Energy Services	Stan T. Rzad	Affirmative	View
1	Lake Worth Utilities	Walt Gill	Affirmative	
1	Lakeland Electric	Larry E Watt	Negative	View
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Negative	View
1	MEAG Power	Danny Dees	Affirmative	View
1	Metropolitan Water District of Southern California	Ernest Hahn	Affirmative	View
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi Woodward	Negative	View
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	View
1	Nevada Power Co.	James McMorran	Negative	View
1	New York Power Authority	Arnold J. Schuff	Negative	
1	North Carolina Electric Membership Corp.	Gary Ofner	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	

1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Douglas G Peterchuck	Affirmative	
1	Oncor Electric Delivery	Michael T. Quinn	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Colt Norrish	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	Frank F. Afranji	Affirmative	View
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch		
1	Rochester Gas and Electric Corp.	John C Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	South Texas Electric Cooperative	Richard McLeon	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	View
1	Southern Illinois Power Coop.	William G. Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	View
1	Southwestern Power Administration	Gary W Cox		
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Affirmative	
1	Transmission Agency of Northern California	James W. Beck	Affirmative	View
1	Tri-State G & T Association, Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	View
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Gregory Van Pelt	Abstain	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Negative	View
2	Independent Electricity System Operator	Kim Warren	Negative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Jason L Marshall	Negative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Negative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana		
3	American Public Power Association	Nathan Mitchell	Abstain	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	Avista Corp.	Robert Lafferty	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Power Agency	Duane S. Dahlquist		
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte		

3	Central Lincoln PUD	Steve Alexanderson	Abstain	View
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	View
3	City of Clewiston	Lynne Mila		
3	City of Farmington	Linda R. Jacobson	Affirmative	View
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	View
3	City of Leesburg	Phil Janik		
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Abstain	
3	ComEd	Bruce Krawczyk	Affirmative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Negative	View
3	Cowlitz County PUD	Russell A Noble	Negative	View
3	CPS Energy	Edwin Les Barrow		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Solutions	Kevin Querry	Affirmative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney		
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	View
3	Georgia Power Company	Anthony L Wilson	Affirmative	View
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier		
3	Hydro One Networks, Inc.	David L Kiguel	Negative	View
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Board of Public Utilities	Robert D Adam	Affirmative	View
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Negative	View
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	View
3	Manitoba Hydro	Greg C. Parent	Negative	View
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	View
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Affirmative	View
3	New York Power Authority	Marilyn Brown	Negative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone		
3	North Carolina Municipal Power Agency #1	Denise Roeder		
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	View
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David T. Anderson	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	Owensboro Municipal Utilities	Richard H. Chapman		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	Vincent J. Catania	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson	Negative	View

3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	View
3	Xcel Energy, Inc.	Michael Ibold		
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Negative	View
4	American Municipal Power - Ohio	Kevin Koloini	Negative	
4	American Public Power Association	Allen Mosher	Abstain	View
4	Central Lincoln PUD	Shamus J Gamache	Abstain	View
4	City of Clewiston	Kevin McCarthy		
4	City of New Smyrna Beach Utilities Commission	Timothy Beyrle	Affirmative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Negative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	View
4	Fort Pierce Utilities Authority	Thomas W. Richards	Affirmative	View
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	View
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	View
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	View
4	LaGen	Richard Comeaux	Negative	View
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Abstain	View
4	National Rural Electric Cooperative Association	Barry Lawson	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Terri Pyle	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Abstain	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Affirmative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	View
4	Seattle City Light	Hao Li	Affirmative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	View
4	Wisconsin Public Power Inc.	Patrick Connors	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	View
5	Allegheny Energy Supply Company, LLC	Robert Loy	Negative	
5	Amerenue	Sam Dwyer	Affirmative	
5	APS	Mel Jensen	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Chelan County Public Utility District #1	John Yale	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Grand Island	Jeff Mead	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Cleco Power	Stephanie Huffman	Abstain	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	View
5	Consumers Energy	James B Lewis	Negative	View
5	Cowlitz County PUD	Bob Essex	Negative	View
5	CPS Energy	Robert B Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	

5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer		
5	East Kentucky Power Coop.	Stephen Ricker	Affirmative	
5	Energy Northwest - Columbia Generating Station	Doug Ramey	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	ExxonMobil Research and Engineering	Martin Kaufman		
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Florida Municipal Power Agency	David Schumann	Affirmative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Green Country Energy	Greg Froehling	Affirmative	
5	Horizon Wind Energy	Brent Hebert	Negative	View
5	Indeck Energy Services, Inc.	Rex A Roehl	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	Thomas J Trickey		
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Louisville Gas and Electric Co.	Charlie Martin		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	View
5	Manitoba Hydro	S N Fernando	Negative	View
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	View
5	MEAG Power	Steven Grego	Affirmative	View
5	Michigan Public Power Agency	James R. Nickel		
5	MidAmerican Energy Co.	Christopher Schneider		
5	Nebraska Public Power District	Don Schmit	Affirmative	View
5	New York Power Authority	Gerald Mannarino	Negative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle DAntuono	Affirmative	View
5	Oglethorpe Power Corporation	Scott McGough	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Jerzy A Slusarz	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Reedy Creek Energy Services	Bernie Budnik		
5	RRI Energy	Thomas J. Bradish	Abstain	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	View
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	George T. Ballew	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	View
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer P.E.	Affirmative	
5	US Power Generating Company	Bohdan M Dackow	Negative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	View
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	AEP Marketing	Edward P. Cox	Affirmative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	View
6	Arizona Public Service Co.	Justin Thompson	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	Cleco Power LLC	Robert Hirchak	Abstain	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entegra Power Services	Larry W. Rodriguez	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	View
6	Florida Municipal Power Pool	Thomas E Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	View
6	Lakeland Electric	Paul Shipps	Negative	View
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Louisville Gas and Electric Co.	Daryn Barker		
6	Luminant Energy	Brad Jones	Affirmative	View
6	Madison Gas and Electric Co.	Jeffrey M Keebler	Abstain	View
6	Manitoba Hydro	Daniel Prowse	Negative	View
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	Missouri River Energy Services	Gerald A. Tielke		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	NRG Energy, Inc.	Alan R. Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson		
6	PPL EnergyPlus LLC	Mark A Heimbach	Abstain	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson		
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	SunGard Data Systems	Christopher K Heisler		
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Joann Wehle		
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Wisconsin Public Service Corp.	Paul Spicer		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
7	Oak Ridge National Laboratory	Stacy Prowell		
8		John Kutzer		
8		Scott Hudson		
8		Roger C Zaklukiewicz	Affirmative	
8		James A Maenner	Negative	
8		Edward C Stein	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski		
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	SPS Consulting Group Inc.	Jim R Stanton	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon		
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	North Carolina Utilities Commission	Kimberly J. Jones		

9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	
10	Southwest Power Pool Regional Entity	Stacy Dochoda	Affirmative	View
10	Texas Reliability Entity	Larry D. Grimm	Affirmative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement
Successive Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Project 2008-06 - Cyber Security Order 706
A successive ballot on revisions to CIP-002 concluded on December 10, 2010.

Ballot Results for Revisions to CIP-002-4
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 87.07 %
Approval: 77.06 %
Since there were negative ballots that included a comment, these results are not final.

Next Steps
The drafting team will post its consideration of all comments (those submitted with a comment form, and those submitted with a ballot) and the standard will proceed to a recirculation ballot.

Background:
FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

The team has been working to revise CIP-002 – Identification of Critical Assets, with the goal of establishing bright line criteria for the identification of critical assets. In November, the SC Executive Committee authorized the team to conduct an abbreviated comment period in parallel with a successive ballot, to support providing stakeholders with the opportunity to provide comment while also supporting the goal of completing this set of revisions to CIP-002 before the end of December, 2010.

Further details are available on the project page:
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Standards Process
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments on Project 2008-06

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

1. **When reviewing the changes to the proposed CIP-002-4 standard, do you believe that the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets?**..... 7

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Janet Smith	Arizona Public Service Company	X		X		X					
2.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				
3.	Group	Mike Garton	Electric Market Policy	X		X		X	X				
4.	Group	Michael Gammon	Kansas City Power & Light	X		X		X	X				
5.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										X
6.	Group	Guy Zito	Northeast Power Coordinating Council										X
7.	Group	Larry Saxon	OGE	X		X		X					
8.	Group	David K Thorne	Pepco Holdings Inc and Affiliates	X		X							
9.	Group	JT Wood	Southern Company Transmission	X		X							

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Paul McClay	Tampa Electric	X		X	X	X					
11.	Individual	Kenneth A. Goldsmith	Alliant Energy				X						
12.	Individual	Kirit Shah	Ameren	X		X		X	X				
13.	Individual	Andrew Pusztai	American Transmission Company	X									
14.	Individual	Dan Klempel	Basin Electric Power Cooperative	X		X		X					
15.	Individual	Bill Keagle	BGE	X									
16.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	X		X		X					
17.	Individual	Steve Alexanderson	Central Lincoln			X	X						
18.	Individual	Jeffrey Mead	City of Grand Island					X					
19.	Individual	John Allen	City Utilities of Springfield, Missouri	X			X						
20.	Individual	Brenda Powell	Constellation Energy Commodities Group						X				
21.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
22.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
23.	Individual	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				
24.	Individual	Marc A. Child	Great River Energy	X		X		X	X				
25.	Individual	Joe Knight	Great River Energy	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
26.	Individual	John Kutzer	Independent Consultant								X		
27.	Individual	Dan Rochester	Independent Electricity System Operator		X								
28.	Individual	Rick Terrill	Luminant					X	X				
29.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
30.	Individual	Jason L. Marshall	Midwest ISO		X								
31.	Individual	Randi Woodward	Minnesota Power	X									
32.	Individual	Joe O'Brien for Tim Conway	NIPSCO	X		X		X	X				
33.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
34.	Individual	Kelsi Oswald	Pinellas County Resource Recovery Facility					X					
35.	Individual	Adam Menendez	Portland General Electric Company	X		X		X	X				
36.	Individual	Barry J Skoras	PPL Electric Utilities Corporation	X									
37.	Individual	Matt Brewer	San Diego Gas and Electric	X		X		X					
38.	Individual	Jim Stanton	SPS Energy								X		
39.	Individual	Scott Amsden	Tacoma Power	X		X	X	X	X				
40.	Individual	andres lopez esquerra	USACE					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
41.	Individual	Louise McCarren	WECC										X
42.	Individual	Candace Morakinyo	Wisconsin Electric Power Company d/b/a We Energies					X	X				

1. When reviewing the changes to the proposed CIP-002-4 standard, do you believe that the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets?

Summary Consideration: In general, most commenters stated that they believed the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets. The following summary of comments and responses is grouped by areas of CIP-002-4.

General Comments:

Concern was expressed that any clarification included in the Guidance Document should be made part of the Standard. The SDT responded that, while the Guidance Documents are not the standard, they do provide additional context. Other entities expressed concern that the bright line prescribed in Attachment 1 will still include smaller Registered Entities that do not have significant impact on the reliable operation of the BES. The SDT responded that in FERC Order 706, the Commission addressed the importance of Critical Assets, no matter how small. Another entity stated that there needs to be a clear and consistent method for Planning to identify IROLs, or it becomes subjective and open to interpretation. The SDT responded that the purpose of FAC-014-2 Requirements R3 and R4 is to establish a clear and consistent method for identifying IROLs. The method for Planning to identify IROLs is beyond the scope of the CIP standards. Several entities expressed an interest that the SDT should take steps to reduce ambiguous language. (e.g. black start resources). The SDT responded that they have made efforts to reduce any ambiguous language, to the point of using the NERC glossary term “Blackstart Resources” in order to eliminate any confusion over the term.

Several entities stated that the SDT should clarify that substations are the facilities to be identified as Transmission Critical Assets, not lines, transformers, reactive equipment, etc. The SDT responded that substations are not the only Facilities identified as Critical Assets. Lines, transformers, reactive equipment, and other Facilities can be classified as a Critical Asset if they meet any of the criteria in Attachment 1. The SDT referred commenters to the posted guidance document for additional clarification. One entity expressed concern that many items give one entity the power to designate facilities owned by another entity as critical. The SDT responded that the issue of communication between entities is recognized as an issue that needs to be addressed and will be considered in a future version. Some entities felt that the SDT was prescriptive in determining Critical Assets, which they felt was contrary to FERC Order 706. The SDT responded that the Attachment 1 criteria were developed in response to an external oversight directive in the FERC Order 706. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This “bright-line” criteria approach removes the variability of entity defined methodologies that would prompt the need for external review. Additionally, some entities expressed concern that the SDT should begin a similar effort in identifying a bright line criteria for Critical Cyber Assets. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method, not the Critical Cyber Asset Identification method.

Nuclear Applicability:

Several entities expressed concern about the nuclear generation exemption language for nuclear generation plants located in the United States (U.S.) along with the parenthetical text of Attachment 1 criterion stating "including nuclear generation." They expressed that this leaves the standard ambiguous and in need of clarification based on recent Nuclear Regulatory Commission (NRC) findings. The NRC and NERC have worked closely to address FERC's Order 706B concerns related to any nuclear balance of plant (BOP) systems, structures and components (SSCs) within a U.S. nuclear power plant that is not regulated by the NRC and subject to NERC CIP standards. However, the NRC letter to NERC dated November 26, 2010 clarifies its findings that "Based on the Commission's [NRC] determination, the NRC staff does not believe that there will be any SSCs in the BOP that will fall under NERC's Critical Infrastructure Protection (CIP) standards." The SDT responded that the phrase "including nuclear generation" in criterion 1.1 is there to define a plant site. Unit output from all units at a single plant site should be included to determine if a plant meets the 1500MW threshold. The evaluation for Critical Cyber Assets is similar. Although it is highly unlikely that nuclear and non-nuclear units share common Cyber Assets, the evaluation should still occur. In addition, the Applicability language has been modified in light of the NRC letter.

Requirement R2:

An entity expressed concern that the requirement as written continues and does not solve the ambiguity with the current Critical Cyber Asset identification requirement. Specifically: "essential to the operation of the Critical Asset" needs to be defined; "adversely impact the reliable operation" needs to be defined; and, it is not clear what "within 15 minutes" means in this context. The SDT responded that the scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The subjectivity involved in the Critical Cyber Asset identification requirement will be addressed in future releases of these Standards. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.

Requirement R3:

An entity expressed concern that the SDT should confirm that under the proposed language for Requirement R3 the approval of the senior manager of the CCA list is only required on an annual basis, and that intermediate updates made "as necessary" under this Requirement do not require senior manager approval. Additionally, the SDT should confirm that under the proposed language for Requirement R3 that the timing of updates "as necessary" to the CCA list is left to the discretion of the entity, and that there is no expectation that such updates are completed within a certain period of time. The SDT responded that the intent of Requirement R3 is that the approval of lists by the senior manager is only required on an annual basis. The intermediate updates do not require senior management approval. The timing of the updates for the Critical Asset list and the Critical Cyber Asset list is not specified and is left to the discretion of the Responsible Entity.

Attachment 1:

Criterion 1.1

One entity expressed concern that criterion 1.1 needs to have "in a single interconnection" added to the end. They provided an example of a single plant site that resided in two Interconnections. The SDT incorporated the suggested wording as clarification of criterion 1.1. Another commenter was concerned about communication that is necessary between various Responsible Entities to identify Critical Assets. The SDT agreed that communication between various Responsible Entities will be required to ensure that all critical Assets are identified. Another commenter stated that the threshold for criteria 1.1, needs to be supported by engineering principles and transmission operations knowledge. The SDT responded that it performed an informal survey of the regions and identified what the megawatt value of the reserve sharing would be for various groups. The SDT used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions.

Criterion 1.2

One commenter expressed that 1000 MVAR was too large, and that there are not any reactive resources that large in their region. They asked if the drafting team is aware of where any 1000 MVAR resources are located. The SDT responded that the survey that NERC conducted earlier this year showed that there were facilities that would qualify at this threshold.

Criterion 1.3

One commenter expressed that criterion 1.3 was not consistent with the goal of providing bright line requirements. This criterion requires entity to conduct a study and submit to the Reliability Coordinator, Planning Coordinator or Transmission Planner, who will then determine if a facility qualifies as critical. The SDT responded that there is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed to avoid Adverse Reliability Impacts in the long-term planning horizon. However, if the PC or TP has identified Adverse Reliability Impacts (the impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection), then any units identified that avoid this scenario must be classified as a Critical Asset. Another entity stated that the term "long-term planning horizon" is referenced but is not clear within the Standard what it means or that it is defined elsewhere. The SDT responded that the resource document “Time Horizons” (found at http://www.nerc.com/files/Time_Horizons.pdf) was used to determine the long-term planning horizon. In this document, long-term planning is defined as “a planning horizon of one year or longer”

One commenter stated that the Reliability Coordinator should be the entity to determine the criticality of a generation Facility, based on information it receives from the Planning Coordinator. The SDT responded that based on the functional model the Planning Coordinator or the Transmission Planner are the correct entities to perform the evaluation. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.

Criterion 1.4

One commenter expressed concern that the Blackstart Resources term used in Criteria 1.4 and 1.5 is in the NERC Glossary and is used in EOP-005-2. However this standard and the related definition are not approved by FERC yet. So what happens if the definition of Blackstart Resource is significantly changed after approval of this standard? The SDT responded that this concern was noted prior to the second posting and the implementation plan was revised to clarify the issue.

Another commenter suggested that NERC consider a “Black Start Tier Methodology” in which only “Primary Black Start Units” would fall under stringent compliance scrutiny and obligations, while other “Secondary Tier Units” would still be made available with required annual testing and operating specifications but be taken off the scope of NERC compliance. The SDT responded that a tiered approach to Blackstart Resources is a good idea, and the SDT suggested that a SAR be submitted by the entity outlining this approach to EOP-005-2.

The APPA CIP Task Force identified what they believed to be an unintended consequence - a Catch-22 - from the interaction of the revised CIP-002-4 Attachment 1’s Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as a Critical Asset. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator’s System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

Criterion 1.5

A few commenters suggested alternate wording for this criterion. The SDT discussed the merits of each, but ultimately decided to keep the posted wording unchanged.

Criteria 1.6 and 1.7

One commenter stated that this criterion should have another factor based on the size of the facility such that loss of the Facility would have an adverse impact on the BES. The SDT will take this suggestion under consideration for future revisions.

Another commenter believed the list of relevant transmission facilities developed by the Responsible Entity should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. Such an arrangement would be akin to the exemption provisions advocated by FERC in its Final Rule on Revisions to the ERO definition of Bulk Electric System. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis.

Criterion 1.8 and 1.9

Several entities asked where the phrase "critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies" came from. The SDT responded that this phrase came from FAC-014-2 Requirement R5. One commenter stated that there should be some obligation that the parties that identify the Transmission Facility as critical also notify the Transmission Owner and Operator of that identification so the Transmission Owner and Operator are aware and can protect. The SDT responded that FAC-014-2 R5 contains information concerning communication of Facilities that are critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

Another commenter expressed that the Reliability Coordinator be removed from the criterion that identifies Critical Asset facilities based on Interconnection Reliability Operating Limits (IROLs). The SDT responded that according to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion.

Another commenter stated that only the Reliability Coordinator develops IROLs, and as such should be the only entity to determine criticality, that the NERC Functional Model Version 5 identifies a Planning Coordinator, not a Planning Authority, and that since the Planning Coordinator is referred to in the standard, it must be included in the Applicability section. The SDT responded that FAC-014-2 Requirement R3 states "The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology." FAC-014-2 Requirement R4 states "The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology." FAC-014-2 Requirement R1 states "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." According to FAC-014-2, the Reliability Coordinator does not develop IROLs. They ensure that the IROLs are established, and that they are consistent with their SOL methodology. Planning Authority is referenced because of FAC-014-2 Requirement R3. Also, since the Planning Coordinator would not own any Critical Assets, they are not subject to CIP-002-4 and would not be listed as a Responsible Entity.

Criterion 1.10

Several commenters stated that the phrase "directly" should be included in Criterion 1.10 which existed in the previous draft. The SDT responded that several commenters in the first posting were concerned about the use of the term "directly." After consideration by the SDT, it was determined that the term could be removed without affecting the intent of the criterion. One commenter expressed concern that, in so much as Criterion 1.1 could result in the identification of generation plant locations with no Critical Cyber Assets, the resulting requirements in Criterion 1.10 could result in expending efforts protecting transmission assets that might not otherwise need to be protected, diverting resources that might be more effectively expended elsewhere. The SDT responded that the intent of Criterion 1.10 is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset.

Criterion 1.11

Several commenters stated that this criterion should either be removed or revised to "Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements." The SDT responded that Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." While the purpose of NUC-001-2 states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown," it is a NERC reliability standard and as such helps to ensure the reliability of the Bulk Electric System.

Criterion 1.13

Several commenters asked that the Guidance Document be modified to provide the reasoning behind the 300 MW criteria listed in criterion 1.13. The SDT responded that the posted Guidance document has been modified to add reasoning for the threshold level. Other commenters suggested alternate wording for the criterion. The SDT discussed the merits of each, but ultimately decided to keep the posted wording unchanged.

Some commenters stated that criterion 1.13 should be reworded to indicate that distributed UFLS or UVLS schemes (i.e., individual UF or UV relays operating independently in multiple substations) are not considered to be a critical asset. Collectively the UFLS or UVLS scheme may shed more than 300MW; however, due to the distributed nature of the scheme, the UFLS or UVLS schemes are not considered to be a critical asset. The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. The SDT responded that a discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. This criterion is intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes.

Criterion 1.15

One commenter asked for clarification on what the term "control" means. The SDT responded that from the posted Guidance document: "A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction." Another entity expressed concern that if a small utility, as a joint owner, has control over only a small portion of a large plant that falls under the brightline of criterion 1.1, they are concerned that as currently written, the first sentence of criterion 1.15 would designate this small utility's control center as critical. The SDT responded that the concern is that the joint owner's control center could provide a path to compromise the functionality of the generation designated a Critical Asset.

Criteria 1.16 and 1.17

One commenter stated that they believe that in Criterion 1.16 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. The SDT responded that due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. Attachment 1 criteria are used to identify control centers as Critical Assets. The consideration of specific reliability functions would be a part of the entity identifying Critical Cyber Assets which support the control center.

Implementation Plan

One entity stated that the proposed implementation is too aggressive. Physical Security Perimeters are expensive and it may not be possible to fund these modifications in the short timeframe for compliance. A 3-year implementation period would be more appropriate. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC Approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Organization	Yes or No	Question 1 Comment
Arizona Public Service Company	Yes	
Dynegy Inc.	Yes	
NIPSCO	Yes	

Organization	Yes or No	Question 1 Comment
Northeast Utilities	Yes	
Portland General Electric Company	Yes	(1) The Standard Drafting Team (SDT) should confirm that under the proposed language for Requirement 1 the approval of the senior manager of the CCA list is only required on an annual basis, and that intermediate updates made "as necessary" under this Requirement do not require senior manager approval.(2) The SDT should confirm that under the proposed language for Requirement 1 that the timing of updates "as necessary" to the CCA list is left to the discretion of the entity, and that there is no expectation that such updates are completed within a certain period of time.
Response: Thank you for your comments. The intent of Requirement R3 is that the approval of lists by the senior manager is only required on an annual basis. The intermediate updates do not require senior management approval. The timing of the updates for the Critical Asset list and the Critical Cyber Asset list is not specified and is left to the discretion of the Responsible Entity.		
Ameren	No	. We suggest Criteria 1.6, 1.7 and 1.10 should be changed to include substations and switchyard (station) only and not “Facilities”. Based on the definition of “Facilities” and application of Criteria 1.6, 1.7 and 1.10, the Critical Asset list now would include transmission lines. Our concern is that there will be significant issue to comply with CIP-003 through CIP-009 (for example, physical security requirements) for the transmission line assets, if some components installed on the lines fall into cyber asset category, such as temperature or flow monitoring devices or fiber optics used for communication. 2. The Blackstart Resources term used in Criteria 1.4 and 1.5 is in the NERC Glossary and is used in EOP-005-2. However this standard and the related definition are not approved by FERC yet. So what happens if the definition of Blackstart Resource is significantly changed after approval of this standard? We suggest that the definition of Blackstart Resources should be included in this standard. 3. The phrase “directly” should be included in Criterion 1.10 which existed in the previous draft. We believe that after removing this term, the revised wordings now are more confusing. 4. We believe that in Criterion 1.16 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. We suggest that Criterion 1.16 should be modified to read “Each control center or backup control center used to perform the functional

Organization	Yes or No	Question 1 Comment
		obligations, pertaining to real time operation of the BES, of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." 5. We believe that in Criterion 1.17 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. Further this criterion should make clear that the 1500 MW is calculated on the same basis as defined in Critetion 1.1. We suggest that Criterion 1.17 should be modified to read, "Each control center or backup control center used to perform the functional obligations, pertaining to real time operation of the BES, of a Balancing Authority if its Balancing Authority Area(s) includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations pertaining to real time operation of the BES, of a Balancing Authority if its Balancing Authority Area(s) includes an aggregate of 1500 MW in a single Interconnection, calculated using the highest rated net Real Power capability of each unit during the preceding 12 months. 6. During the Webinar, references were made to the Guidance Document. However, the Guidance Document is NOT the standard and can not be used in the compliance audit. So, any clarification included in the Guidance Document should be made part of the Standard.

Response: Thank you for your comments.

1. The SDT does not feel this change is necessary. Please refer to the first bullet in the Overall Application of Attachment 1 in the posted Guidance document for a discussion of the SDT's reason for the use of the term "Facility."
2. Your concern was noted prior to the second posting and the implementation plan was revised with the following: "The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities." The language has been revised in this posting to "The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted to FERC for regulatory approval in the US with Project 2006-03 – System Restoration and Blackstart. The Effective Date of EOP-005-2 is the date that Criteria 1.4 and 1.5 will be used to determine Critical Assets for any Responsible Entity."
3. Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion.
4. Due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical

Organization	Yes or No	Question 1 Comment
		Assets. Attachment 1 criteria are used to identify control centers as Critical Assets. The consideration of specific reliability functions would be a part of the entity identifying Critical Cyber Assets which support the control center. 5. Due to the direct impact on the operation of identified Critical Assets, these Balancing Authority control centers must be designated as Critical Assets. The impact to the identified Critical Assets would be in real time, as the Balancing Authority functions in the Functional Model involve real time operations. If a Balancing Authority can control 1500MW or more of generation, it is considered a Critical Asset. The language in criterion 1.1 was taken from MOD-024, which is only applicable to Generation Owners. 6. While the Guidance Documents are not the standard, they do provide additional context. The SDT believes the wording in the posted standard provide sufficient clarity.
Kansas City Power & Light	No	o The bright line prescribed here will still include smaller Registered Entities that do not have significant impact on the reliable operation of the BES. The bright line components that need to be considered for modification are those regarding control centers and the blackstart facility considerations. It may be easiest to consider the role system load could play in the entirety of this bright line. For example, leave the bright line language as is, but those entities with 500 MW of system load or less are exempt. o Section 1.8 is not clear as to the intent. If the intent is to include those facilities that are identified as IROL flowgates then it is recommended the Drafting Team consider the following language, "Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as a LODF flowgate with an IROL limit established and the associated contingent facility(ies)." If this is not the case what does, "critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies" mean? o Section 1.9 is not clear as to the intent for the same reasons stated for section 1.8. If the intent is to include those facilities that are identified as IROL flowgates then it is recommended the Drafting Team consider the following language, "Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as a LODF flowgate with an IROL limit established and their associated contingent facility(ies). If this is not the case what does, "critical to the derivation of Interconnection

Organization	Yes or No	Question 1 Comment
		Reliability Operating Limits (IROLs) and their associated contingencies" mean?
Response: Thank you for your comments. • In FERC Order 706, the Commission addressed the importance of Critical Assets, no matter how small. An entity with 500MW or less of system load may still have a Critical Asset which needs to be evaluated for possible Critical Cyber Assets. • The wording for criterion 1.8 came from FAC-014-2 Requirement R5. • The wording for criterion 1.9 came from FAC-014-2 Requirement R5.		
Great River Energy	Yes	After reviewing the SDT summary of comments and their associated edits to Attachment 1, GRE feels the changes were responsive to the feedback received by industry in the previous comment/ballot period.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment.		
Alliant Energy	No	Alliant Energy agrees with most of the changes to the standard, however, Attachment 1, Criterion 1.4 concerning Blackstart Resources is unacceptable as currently written. Alliant Energy fears that there will be a degradation of the Black Start program as it exists today. The industry has already seen companies removing their black start resources from Power System Restoration Plans due to compliance requirements which entail additional costs associated with not only bringing these units up to the required standards but the extensive fines which may occur if rigid compliance specifications are not met. We would respectfully suggest that NERC consider a "Black Start Tier Methodology" in which only "Primary Black Start Units" would fall under stringent compliance scrutiny and obligations, while other "Secondary Tier Units" would still be made available with required annual testing and operating specifications but be taken off the scope of NERC compliance. This methodology would promote back up facilities to the primary black start units and would encourage smaller black start units to remain in the black start program which could be used to expedite the restoration process. A "Black Start Area Plan" could be created to specify the "Primary Black Start Units" and "Secondary Black Start Units" requirements for a given footprint or specified loading area. A minimum of one "Primary Black Start Unit" would be required for any specific footprint with special additional considerations for those units which may supply stabilization power to nuclear facilities. The Black Start Tariff could be utilized to maintain the "Primary Black Start Units" availability and be used to reward the availability of the "Secondary Black Start Units". The tariff could also be used by those entities which do not physically have such facilities but could contract to support this kind of services. A third possible tier of black start units could be defined and incorporated which would be comprised of larger coal/gas units with only black start stabilization capability. Incorporating these third tier units would enable coal/ gas units to self supply their own stabilization power and would be immediately made available to contribute to the loading and stabilization of the black start area plan once the skeletal grid was reconstructed. These types of units could also be rewarded through the black start tariff to ensure unit availability, and promote the reduction of unit damage which can occur to generating stations during a black out situation.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments. A tiered approach to Blackstart Resources is a good idea, and the drafting team suggests that a SAR be submitted by the entity outlining this approach to EOP-005-2. It is beyond the scope of this SDT.		
American Transmission Company	No	ATC believes that Attachment 1, the so-called bright line criteria, language needs to be clarified. There needs to be a clear and consistent method for Planning to identify IROLs, or it becomes subjective and open to interpretation. The following are ATC's recommended changes to the Criteria listed: Criterion 1.3: o Not consistent with the goal of providing bright line requirements. This criterion requires entity to conduct a study and submit to the RC, PC or TP, who will then determine if a facility qualifies as critical. These criteria will likely result in inconsistent and unrepeatable studies being performed by RC, PC or TP. Comment also applies to 1.8, 1.9. o Suggestion: Delete this criterion at the next CIP-002 revision. Criterion 1.8: o The 'critical to the derivation of . . . and their associated contingencies' wording is more cryptic and less clear than the previous wording. o Suggestion: Suggest wording more similar to the previous draft, 'Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs.' Criterion 1.10: o We suggest expanding the wording of "loss of the assets" to "loss of more than 1500 MW of assets" to clarify that the inclusion of Transmission Facilities that would result in the loss of more than 1500 MW but less than all of the assets at a single plant location and the exclusion of Transmission Facilities that may result in the loss of less than 1500 MW of the assets at a single plant location. o Added the wording of 'identified by any Generator Owner as a result of its application of'. Generator Owner would apply Criterion 1.1 and 1.3 to its generating facility, rather than obligate the TO to apply the criteria which and possibly lead to disagreements. Criterion 1.11: o This criterion is not clear and distinct because in an ultimate analysis the entire interconnection minus certain selected elements is essential to meeting the NPIRs at any given nuclear facility. o Suggestion: Revise the criterion to, "Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements", which is consistent with the

Organization	Yes or No	Question 1 Comment
		former EEI comments.

Response: Thank you for your comments.

The purpose of FAC-014-2 Requirements R3 and R4 is to establish a clear and consistent method for identifying IROLs. The method for Planning to identify IROLs is beyond the scope of the CIP standards.

Criterion 1.3: There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed to avoid Adverse Reliability Impacts in the long-term planning horizon. However, if the PC or TP has identified Adverse Reliability Impacts (the impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that

Organization	Yes or No	Question 1 Comment
affects a widespread area of the Interconnection), then any units identified that avoid this scenario must be classified as a Critical Asset. Criterion 1.8: The wording for criterion 1.8 came from FAC-014-2 Requirement R5. Criterion 1.10: The SDT believes the phrase "loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3" contained in the balloted version of CIP-002-4 conveys the same intent as your proposed language. Criterion 1.11: Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs."		
Basin Electric Power Cooperative		Attachment #1, Criterion 1.1 needs to have "in a single interconnection" added to the end. The Laramie River Station in Wheatland, Wyoming is a three generator station with two 550 MW generators in the Western Interconnection and one 550 MW generator in the Eastern Interconnection. (there doesn't appear to be any specific place to submit substantative comments on the standard)
Response: Thank you for your comments. The SDT has incorporated your suggested wording in Attachment 1 Criterion 1.1.		
Pepco Holdings Inc and Affiliates	Yes	Attachment 1 Critical Asset CriteriaItem 1.1-- Please clarify the process that the Transmission Owner would find out about Generator Owners or Generator Operator facilities identified under Item 1.3. Suggest have some statement similar to 1.3 regarding informs. Should the Planning Coordinator or Transmission Planner not only designate and inform the Generator Owner or Generator Operator but the Transmission Owner?General-- Please take steps to reduce ambiguous language. (e.g. black start resources).
Response: Thank you for your comments. Criterion 1.3: The process would be that the Planning Coordinator or Transmission Planner would notify the Generation Owner and Generation Operator about any facilities that meet Criterion 1.3. The GO and/or GOP would need to notify the Transmission Owner of any facilities that need to be considered for Criterion 1.10. The SDT has made efforts to reduce any ambiguous language. In your example the SDT chose the NERC glossary term "Blackstart Resources" in		

Organization	Yes or No	Question 1 Comment
order to eliminate any confusion over the term.		
BGE	Yes	BGE thanks the SDT for their positive response to the previously submitted comments. BGE asks that the SDT consider adding to the Guidance Document the reasoning behind the 300 MW criteria listed in the automatic load shedding criteria 1.13 in Appendix 1.
Response: Thank you for your comments. The posted Guidance document has been modified to add reasoning for the threshold level.		
Bonneville Power Administration	No	BPA believes that the bright line criteria approach in CIP-002-4 is an improvement over prior versions. However, it still does not address the concern by the industry in regards to providing sufficient clarity to many portions of CIP-002-4 to make it acceptable to the majority of utilities that must understand and develop strategies to meet the standards and requirements and implement them in a reasonably timely fashion. BPA still supports the formal comments that we submitted in October 2010. See additional comments below: CIP-002-4 R2.1. “The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter” does not go far enough in its definition of what qualifies as a critical cyber asset and needs further clarification, particularly concerning serial devices. For example: What exactly is meant by "uses a routable protocol to communicate outside the Electronic Security Perimeter"? 1. Can a device that is not capable of native routable protocol (does not have, or use an ethernet card) qualify as using routable protocol? 2. Does a device that is not capable of native routable protocol, that is connected to a device which is ethernet connection outside the ESP (Serial to Ethernet Converter) qualify? 3. Does a device that is not capable of native routable protocol, but is connected to a Terminal Server, which is ethernet connected outside the ESP qualify?4. Does it make a difference if there is only view access to the internal ESP device with no possible ability to control it?5. What if the device

Organization	Yes or No	Question 1 Comment
		is connected to another device which is ethernet connected, but it simply dumps to a data-store on that device, and there is no access through to the data-store device (the internal ESP device)?6. What if the device itself never initiates communications outbound, and can only be connected to if access is initiated to it from elsewhere?7. What if the device has no ability to connect to and influence any other device?8. What if you can't connect to that device and through it connect to any other device?9. What if the Serial to Ethernet device between the Cyber Asset and the network strips all routable protocol information off and forwards only non-routable data to the Cyber Asset. Comments from October 2010: Mapping Document - The individual utility's development and implementation of their risk-based methodology instills ownership in their process and is a positive result of the current CIP versions. For BPA, application of the bright-line assessment criteria for Critical Asset identification in the recent NERC data request resulted in fewer assets being classified in the high impact categorization. However, we see that if a utility's implementation of the criteria resulted in more Critical Assets being identified with the corresponding implementation of security controls at those assets, then an improvement in reliability would occur. Attachment 1 - Make it clear that substations are the facilities to be identified as Transmission Critical Assets, not lines, transformers, reactive equipment, etc. Another alternative would be to identify all facilities that operate at a specified certain kV level would be determined to be Critical Assets. The different categories identified in Attachment 1still allow utilities to justify most of what they have already declared as Critical Assets. R1 - We agree with the "at least annually" aspect of the requirement. Annual review seems appropriate if a utility has not had any major changes or expansion to their grid since their last Critical Asset determination. R2 - The requirement as written continues and does not solve the ambiguity with the current Critical Cyber Asset identification requirement. Specifically: "essential to the operation of the Critical Asset" needs to be defined; "adversely impact the reliable operation" needs to be defined; and, it is not clear what "within 15 minutes" means in this context. The intent of the Standards Drafting Team needs to be

Organization	Yes or No	Question 1 Comment
		made clear. Implementation Plan - If this version requires more substations to be identified as Critical Assets, then we believe that the proposed implementation is too aggressive. Physical Security Perimeters are expensive and it may not be possible to fund these modifications in the short timeframe for compliance. A 3-year implementation period would be more appropriate. BPA agrees with the proposed revisions to the implementation plan for newly identified CCAs and Responsible Entities.

Response: Thank you for your comments

Requirement R2: This language has existed in versions 1 through 3 of CIP-002. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Also, please refer to the "Identifying Critical Cyber Assets" document for additional clarification.

Mapping Document - While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets in North America will be classified as Critical Assets.

Attachment 1 - Substations are not the only Facilities identified as Critical Assets. Lines, transformers, reactive equipment, and other Facilities can be classified as a Critical Asset if they meet any of the criteria in Attachment 1. Please refer to the posted guidance document for additional clarification.

R2 - The scope of changes to this Standard only addresses the near-term issues associated with external oversight and review of the risk-based assessment methodology. The subjectivity involved in the Critical Cyber Asset identification requirement will be addressed in future releases of these Standards. The 15 minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do

Organization	Yes or No	Question 1 Comment
not necessarily involve real-time reliability impact. Implementation Plan - The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC Approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.		
Brazos Electric Power Cooperative, Inc.	No	Brazos Electric appreciates the work of the SDT and is supportive of the efforts and the general concepts of this draft. This is a negative vote due to disagreement over some elements in Attachment 1 criterion as provided below. 1.3 The term "long-term planning horizon" is referenced but is not clear within the Standard what it means or that it is defined elsewhere. 1.5 This criterion should be clarified by changing the words "first interconnection point of the generation unit(s)to be started" to be "interconection point to the first generation unit(s)to be started". 1.6 This criterion should have another factor based on the size of the facility such that loss of the Facility would have an adverse impact on the BES. 1.7 This criterion should have another factor based on the size of the facility such that loss of the Facility would have an adverse impact on the BES. 1.13 Consider re-wording of this criterion as follows to better intent. “Each system or Facility that performs automatic load shedding as required by regional load shedding programs that implement Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) of 300 MW or more without human operator initiation.” 1.15 This criterion should be clarified to define what the term "control" means. It is not clear within the

Organization	Yes or No	Question 1 Comment
		Standard what it means or that it is defined elsewhere.

Response: Thank you for your comments.

Criterion 1.3 - The resource document "Time Horizons" (found at http://www.nerc.com/files/Time_Horizons.pdf) was used to determine the long-term planning horizon. In this document, long-term planning is defined as "a planning horizon of one year or longer"

Criterion 1.5 - The SDT appreciates the suggestion, but believes the posted wording is adequate.

Criterion 1.6 - The SDT will take this suggestion under consideration for future revisions.

Criterion 1.7 - The SDT will take this suggestion under consideration for future revisions.

Criterion 1.13 - The SDT appreciates the suggestion, but believes the posted wording is adequate.

Criterion 1.15 - From the posted Guidance document: "A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction."

Organization	Yes or No	Question 1 Comment
Central Lincoln	No	Central Lincoln supports the following APPA CIP Task Force comments. If this issue is addressed as suggested, we will vote affirmative on the next ballot. The APPA CIP Task Force has identified what we believe to be an unintended consequence - a Catch-22 - from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size.EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets.Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW).Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size.Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW).In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets.To address this problem, we propose the following edits to 1.4 and 1.5 shown in CAPS:1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart

Organization	Yes or No	Question 1 Comment
		Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation - and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)

Response: Thank you for your comment.

The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as a Critical Asset. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with

Organization	Yes or No	Question 1 Comment
neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.		
City Utilities of Springfield, Missouri	No	City Utilities of Springfield, Missouri believes that the proposed bright-line criteria will improperly identify lower impact Blackstart Resources as Critical Assets. City Utilities agrees with the comments submitted by the APPA Task Force.
Response: Thank you for your comments. Please refer to the response to APPA's Task Force contained in Central Lincoln's comments.		
San Diego Gas and Electric	Yes	Comment on 1.8, 1.9, 1.10: There should be some obligation that the parties that identify the Transmission Facility as critical (e.g. RC, PA, TP, GO) that they also notify the Transmission Owner and Operator of that identification so the TOP and TO are aware and can protect.Comment on 1.8, 1.9: What does the statement "critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies" mean?
Response: Thank you for your comments. Criterion 1.8 and 1.9 - FAC-014-2 R5 contains all of the information concerning communication of Facilities that are critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. Criterion 1.10 – It is agreed that communication between Generator Operators and Transmission Owners and Transmission Operators will be required to ensure that all Critical Assets are identified. The wording for 1.8 and 1.9 came from FAC-014-2 Requirement R5.		

Organization	Yes or No	Question 1 Comment
Electric Market Policy	Yes	Dominion supports the latest revision of CIP-002-4 through CIP-009-4 (excluding CIP-005-4)
Response: Thank you for your comments.		
FirstEnergy	Yes	FirstEnergy agrees that the standard drafting team's changes to the proposed CIP-002-4 reliability standard have been responsive to industry feedback and believe the team's work will drive further consensus. While FE has voted in support of the standard, we offer the following comments as clarifying revisions permitted by the NERC Process Manual prior to a Recirculation (Final) Ballot.A) Applicability to nuclear generation. The proposed revisions regarding exemption language for nuclear generation plants located in the United States (U.S.) along with the parenthetical text of Attachment 1 criterion stating "including nuclear generation" leaves the standard ambiguous and in need of clarification based on recent Nuclear Regulatory Commission (NRC) findings. The NRC and NERC have worked closely to address FERC's Order 706B concerns related to any nuclear balance of plant (BOP) systems, structures and components (SSCs) within a U.S. nuclear power plant that is not regulated by the NRC and subject to NERC CIP standards. However, the NRC letter to NERC dated November 26, 2010 clarifies its findings that "Based on the Commission's [NRC] determination, the NRC staff does not believe that there will be any SSCs in the BOP that will fall under NERC's Critical Infrastructure Protection (CIP) standards." While the letter acknowledges that there may be some SSCs in a nuclear plant that are not subject to the NRC's cyber security regulations or NERC's CIP standards, the NRC indicates "these SSCs do not have a nexus to radiological health and safety and do not affect grid reliability." Based on the NRC's November 26, 2010 FE believes that NERC should retain the original exemption language related to U.S. nuclear plants in section 4.2 of the standard and remove the parenthetical text "including nuclear generation" from the Attachment 1 criteria 1.1.B) Attachment 1, Criterion 1.6. Item 1.6 currently reads "Transmission Facilities operated at 500 kV or higher." For consistency with other Attachment 1 criteria we propose that this criterion be revised to read "Transmission Facilities at a single station or substation location operated at 500kV or higher". This change clarifies that the intent is to classify the 500kV substation as a Critical Asset and not individual transmission lines that terminate at the substation. C) Attachment 1, Criterion 1.8. FirstEnergy suggests that the Reliability Coordinator be removed

Organization	Yes or No	Question 1 Comment
		from the criterion that identifies Critical Asset facilities based on Interconnection Reliability Operating Limits (IROLs). For consistency with criterion 1.3 which identifies Critical Asset generation necessary to avoid BES Adverse Reliability Impacts in the "long-term planning horizon" we propose that the Critical Assets identified based on IROL also be limited to the study of the Planning Coordinator and the Transmission Planner in the long-term planning horizon. The Reliability Coordinators role in real-time conditions for IROL are generally aimed at fine tuning the appropriate operating limits that they monitor based on actual system conditions and would typically not identify any new "facilities" associated with an IROL. In the unlikely event that a Reliability Coordinator would identify a very unique IROL condition not identified by the rigorous study work of a Planning Coordinator or Transmission Planner it would be for extremely unique and temporary system conditions and would not warrant long-term Critical Asset determinations.
Response: Thank you for your comments. Nuclear generation applicability - The phrase "including nuclear generation" in Criterion 1.1 is there to define a plant site. Unit output from all units at a single plant site should be included to determine if a plant meets the 1500MW threshold. The evaluation for Critical Cyber Assets is similar. Although it is highly unlikely that nuclear and non-nuclear units share common Cyber Assets, the evaluation should still occur. Criterion 1.6 – The purpose of classifying Critical Assets is to identify all Critical Cyber Assets. While it is true that almost all Critical Cyber Assets associated with 500kV Facilities are located inside of a substation, the potential exists for it to not be located there. If a Critical Cyber Asset is not located within the bounds of a station or substation, it must still be protected from cyber attacks. Criterion 1.8 – According to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion.		
Tacoma Power	Yes	For Criterion 1.13, the term "System" is defined in the NERC Glossary of Terms but is not capitalized. I suggest that a change be made to capitalize the word System.
Response: Thank you for your comments. The term "system" can refer to systems other than "a combination of generation, transmission, and		

Organization	Yes or No	Question 1 Comment
distribution components." The SDT believes it is correct to refer to "system" instead of "System."		
City of Grand Island	No	General Comment: So many items give one entity the power to designate facilities owned by another entity as critical. Yet there is no mention of justification and no process to mediate differences of opinion. Specific Comments: 1.3 This criteria should have a MW level. Suggest: "Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than 1500 MW." 1.4 Reference Blackstart Resourses identified in 1.4 (see above modified 1.4).
Response: Thank you for your comments. The issue of communication between entities is recognized as an issue that needs to be addressed and will be considered in a future version. Criterion 1.4 - Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as a Critical Asset.		
Pinellas County Resource Recovery Facility	Yes	I think the bright-line criteria provide much needed consistency and give beneficial direction to registered entities in identifying their critical assets.
Response: Thank you for your comment.		

Organization	Yes or No	Question 1 Comment
Independent Consultant	Yes	In CIP-002-4 Attachment 1 Criteria items 1.15 & 1.17 contain two criteria each. The first criteria in each of these statements if based on 'functionality', and the second criteria is based on 'span of control' (> 1500MW). It would appear that a separate criteria for span of control should be listed and that aspect of the criteria removed from 1.15 & 1.17.Suggested separation provided below. Criteria numbering would need to be adjusted appropriately.1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator. 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4.NEW: Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. 1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12. 1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. NEW: Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.
Response: Thank you for your comment. The SDT decided to group the criteria for control centers based on functionality. Separating then does not appear to add any additional clarity to the criteria.		

Organization	Yes or No	Question 1 Comment
Luminant	Yes	Luminant thanks the SDT for their work on the standard and for the opportunity to provide comments for consideration by the SDT. Luminant believes the changes to CIP-002-4 are responsive to the concerns expressed by the industry and provide acceptable bright-line criteria for the determination of Critical Assets. Luminant does request the SDT to consider a wording change in the "Draft Guidance Document". On page 10 of the Clean version of the document, in reference to Special Protection Schemes, the following is listed:"Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time they are required or if they operate outside of the parameters they were designed for. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets. " The term "implemented" is not consistent with other NERC standards and can lead to disagreements on who is responsible for the Critical Asset CIP requirements. Luminant asks the SDT to change the language to: "Generator Owners and Operators that own such systems and schemes...." The term "own" is consistent with other NERC standards that are applicable to Special Protection Systems and Remedial Action Schemes, and very clearly identifies the responsible entity. Thank you for your consideration of our comments.
Response: Thank you for your comments. Your suggested change to the Guidance document has been made.		
Minnesota Power	No	Minnesota Power believes that CIP-002-4 R1 needs to clearly state "The RE should identify a list of Critical Asset that it owns..." While the Standard Drafting Team did speak to this in its response to the California ISO's comments, the SDT did not go far enough to eliminate potential interpretation issues in the future. Specifically, there is ambiguity as to what this would mean from a Balancing Authority perspective. The "its assets" language as written could be interpreted to mean the assets it controls, rather than those assets it owns. As such, we would urge the Standard Drafting Team to reconsider, and include a stronger ownership statement in the proposed standard language.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. The drafting team believes the phrase "a list of its identified Critical Assets" in R1 specifies ownership of the Critical Asset by the Responsible Entity.		
PPL Electric Utilities Corporation	Yes	PPL Electric Utilities Corporation ("PPL EU") appreciates the hard work and efforts of the Standards Drafting Team in reaching this point in the standards development process. However PPL EU has reviewed the CIP-002-4 standard version dated 11/30/2010 and the associated Rationale and Implementation Reference Document and Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and still find the need to offer comments as follows: 1) CIP-002-4, Attachment 1, Criterion 1.1 should include a requirement that the Generator Owner or Generator Operator must inform the Transmission Operator, Transmission Operator, Planning Coordinator or Transmission Planner of each group of generating units that has been designated as a critical asset. 2) CIP-002-4, Attachment 1, Criterion 1.3 should be reworded to indicate "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, "and the Transmission Owner and Transmission Operator" as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon. 3) CIP-002-4, Attachment 1, Criterion 1.5 should be reworded to indicate "The facilities comprising the Cranking Paths and Meeting the initial switching requirements from the Blackstart Resource "up to and including" the first interconnection point of the generation unit(s) to be started, or up to "and including" the point on the Cranking Path where two or more path options exist "including the first interconnection point of the generation unit(s) to be started" , as identified in the Transmission Operator's restoration plan. 4) CIP-002-4, Attachment 1, Criterion 1.13 should be revised to include load shed systems capable of shedding 300 MW or more. These load shed systems, which are typically part of the energy management systems, are initiated to ensure the reliability of the BES. 5) CIP-002-4, Attachment 1, Criterion 1.13 should be reworded to indicate that distributed UFLS or UVLS schemes (i.e., individual UF or UV relays operating independently in multiple substations) are

Organization	Yes or No	Question 1 Comment
		not considered to be a critical asset. Collectively the UFLS or UVLS scheme may shed more than 300MW; however, due to the distributed nature of the scheme, the UFLS or UVLS schemes are not considered to be a critical asset.

Response: Thank you for your comments.

Criterion 1.1 - It is agreed that communication between Generator Operators and Transmission Owners and Transmission Operators will be required to ensure that all Critical Assets are identified.

Criterion 1.3 - The process would be that the Planning Coordinator or Transmission Planner would notify the Generation Owner and Generation Operator about any facilities that meet Criterion 1.3. The GO and/or GOP would need to notify the Transmission Owner of any facilities that need to be considered for Criterion 1.10.

Criterion 1.5 - The SDT appreciates the suggestion, but believes the posted wording is adequate.

Criterion 1.13 – A discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. During the previous ballot and comment period, the SDT received many comments on this criterion, whose wording was similar to this suggestion. Some commenters stated that the wording of this criterion will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate “like” systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems “configured” for automatic load shedding, not simply just “capable” of load shedding. This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. The SDT appreciates the suggestion, but believes the posted wording is correct.

Organization	Yes or No	Question 1 Comment
Southern Company Transmission	Yes	Southern believes that the SDT's changes to the proposed standard were responsive to some of the feedback received; however, certain key industry comments still have not been adequately addressed. For example, in Attachment 1, Section 1.11 should be deleted. Section 1.11 relates to Transmission Facilities necessary to secure offsite power to permit safe reactor shutdown. Although such Transmission Facilities are within the scope of Nuclear Plant Interface Coordination standards (NUC reliability standards), they are not within the intended scope of the Cyber Security standards (CIP reliability standards). The Purpose section of the NUC reliability standards states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown." The Purpose section of the CIP reliability standards states "NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System." Therefore, Section 1.11 should be deleted because it is clearly out of scope. Moreover, the criticality of facilities for BES reliability purposes should not be based on fuel type alone. In addition, Southern believes the following proposed changes made by the SDT should be reconsidered: In Attachment 1, Section 1.10, the SDT deleted the word "directly" by changing "generation interconnection required to directly connect generator output" to "generation interconnection required to connect generator output." The word "directly" should not be deleted from Section 1.10 because it is necessary to appropriately define the scope of the requirement. Removing the word "directly" removes the bright line criteria, which is the goal of the new standard. As proposed by the SDT, the standard would require various risk-based analyses i.e. load flow and transient stability studies to determine the assets in scope. Therefore, the SDT should reconsider this proposed change. The proposed Section 1.13 would be clearer if it were changed to the following: "1.13. Each system or facility that implements Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) of 300 MW or more without human operator initiation as required by the regional load shedding program."

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments. Criterion 1.11 – This criterion is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC reliability standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. While the purpose of NUC-001-2 states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown," it is a NERC reliability standard and as such helps to ensure the reliability of the Bulk Electric System. Criterion 1.10 - Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion. Criterion 1.13 - The SDT appreciates the suggestion, but believes the posted wording is adequate.		

Organization	Yes or No	Question 1 Comment
MRO's NERC Standards Review Subcommittee	No	The MRO NSRS believes the SDT was responsive to much of the feedback received from the industry; however, we question whether these bright-line criteria as a whole are acceptable for determining Critical Cyber Assets. We believe the following criteria need to be adjusted as follows to properly address these areas: Attachment 1, Criterion 1.4We believe EOP-005-2, which defines the Transmission Operator restoration plan and related Blackstart Resource requirements, is ambiguous as to what actually constitutes a Blackstart Resource. For example, assume a plant has a 1 MW diesel engine that is used to start a 100 MW combustion turbine when the system is black. What is the Blackstart Resource, the 1 MW diesel engine or the 100 MW combustion turbine? To our knowledge, EOP-005-2 does not answer this question. Even at the regional restoration plan level, we believe many utilities are currently designating the 1 MW diesel engine as the Blackstart Resource under EOP-005-2, whereas others have designated the 100 MW combustion turbine. We realize this appears to be more of an issue with EOP-005-2, and not CIP-002-4. However, the effect of this EOP-005-2 ambiguity will be greatly magnified once CIP-002-4 begins using this same designation to identify critical assets, determining where an entity focuses their time and resources related to cyber security. For this reason, we believe the CIP-002-4 and EOP-005-2 SDT's must work together to clarify this designation, enabling us to apply the definition of a Blackstart Resource, and the related cyber security efforts, uniformly across the industry. Attachment 1, Criteria 1.4 & 1.5The APPA has identified an issue where criteria 1.4 and 1.5 end up requiring nearly all control centers to be identified as critical, even for small entities. The MRO NSRS recognizes this unintended consequence, and supports the following APPA comments: "The APPA CIP Task Force has identified what we believe to be an unintended consequence - a Catch-22 - from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a

Organization	Yes or No	Question 1 Comment
		critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in quotation marks:"1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan." This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation - and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control

Organization	Yes or No	Question 1 Comment
		centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project. (CIP-002-5 or CIP-010/011)" Attachment 1, Criterion 1.10If a generating facility that falls under the brightline of criterion 1.1 has numerous Transmission Facilities providing interconnections to the system, all of them would be designated as critical under criterion 1.10, even if their loss does not result in the loss of at least 1500 MW of generation. To prevent this, we would propose rewording the criterion as follows:"Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in THE LOSS OF AT LEAST 1500 MW OF GENERATION ASSETS IDENTIFIED BY AN GENERATOR OWNER AS A RESULT OF ITS APPLICATION OF ATTACHMENT 1, CRITERION 1.1, OR the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.3." Attachment 1, Criterion 1.13We are concerned that as currently worded, this criterion could unintentionally designate multiple smaller, disparate systems with like settings as a "system" that performs automatic load shedding of 300 MW or more, assuming the total combined load shedding capability of the disparate systems exceeds 300 MW. To prevent this, we would propose rewording the criterion as follows to more closely match the old version:"Each COMMON system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program." Attachment 1, Criterion 1.15Even if a small utility, as a joint owner, has control over only a small portion of a large plant that falls under the brightline of criterion 1.1, we are concerned that as currently written, the first sentence of criterion 1.15 would unintentionally designate this small utility's control center as critical. To prevent this, we would propose rewording the criterion as follows:"Each control cen

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments Criterion 1.4 - A Blackstart Resource is defined as "A generating unit(s) and its associated set of equipment which has the ability to be started without support from the System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." It is difficult to imagine a scenario in which a 1 MW generator can fulfill all of the requirements in the Blackstart Resource definition. However, any generator designated a Blackstart Resource per EOP-005-2 must be classified a Critical Asset. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as a Critical Asset. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2. Criterion 1.10 - The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. Criterion 1.13 - In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. It is unclear how adding the term "common" adds any additional clarity over the existing wording. A discrete component that sheds more than 300MW of load due to		

Organization	Yes or No	Question 1 Comment
the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. Criterion 1.15 - The concern here is that the joint owner's control center could provide a path to compromise the functionality of the generation designated as a Critical Asset.		
Manitoba Hydro	No	The SDT addressed some but not all of the issues in the current proposed version of CIP-002-4. Please see Manitoba Hydro's voting recommendation and associated comments for further details.
Response: Thank you for your comments.		
USACE	No	The Standards Drafting Team still is been prescriptive in determining Critical Assets. The Responsible Entity is responsible for identifying Critical Assets, as pointed out in Order 706, and FERC directed NERC to provide additional guidance in helping the Responsible Entity determine Critical Assets and for NERC to maintain flexibility for the Responsible Entity in the determination of Critical Assets. The prescriptive nature of the approach being used in the Ver 4 CIP Standard appears to be taking the responsibility of determining Critical Assets away from the Responsible Entity and the lack of flexibility may eliminate or preclude a system or component from being identified as a Critical Asset. This process, with out the jpropper full ris assesment to understand what is critical in the BES system, willnot result on a more secure BES. More assets in the list does not translate to more secure overall system.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The Attachment 1 criteria were developed in response to an external oversight directive in the FERC Order 706. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This "bright-line" criteria approach		

Organization	Yes or No	Question 1 Comment
removes the variability of entity defined methodologies that would prompt the need for external review.		
Constellation Energy Commodities Group	No	The team was very responsive to feedback and addressed each comment. However, we do not believe the bright-line criteria to be acceptable - specifically 1.15. Comments were included on the ballot. In addition, we offer the comment below. New Language - 1.13 - Each system(s) or facilities that perform automatic load shedding, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) as required by the regional load shedding program. Excluding high-set underfrequency load shedding ("UFR"), as incorporated in the ERCOT Load acting as a Resource ("LaaR") Demand Response Program, which requires such relay protection. As the trip threshold for UFR is set above that of the regional requirements for the UFLS, the UFR type load shedding should be exempt from this requirement. (This should be clarified in the Guidance Document to maintain a clear scope of intent in the requirement.)
Response: Thank you for your comment. Criterion 1.13 – If the trip threshold for UFR is set above that of the regional requirements for the UFLS, then the Standard Drafting team is unclear how it would be required as part of the regional UFLS program, and thus be classified as a Critical Asset. The "LaaR" is not part of the regional load shedding program, but an ancillary services market.		

Organization	Yes or No	Question 1 Comment
Northeast Power Coordinating Council	No	The wording in the Applicability Section exempts "Facilities regulated by the Canadian Nuclear Safety Commission", and "Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54." It is stated in 1.1 "(including nuclear generation)...", contradicting the Applicability section. Criteria 1.3 as revised--"Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon." From the NERC Functional Model, the Reliability Coordinator should be the entity to determine the criticality of a generation Facility, based on information it receives from the Planning Coordinator. Criteria 1.8 as revised--"Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." As per the NERC Functional Model, only the Reliability Coordinator develops IROLs, and as such should be the only entity to determine criticality. There is no need to say "substation location"--substation or station will suffice. Where more than one entity is listed (such as Reliability Coordinator, Planning Coordinator, et al., it must be made clear which of those entities is the primary entity. The NERC Functional Model Version 5 identifies a Planning Coordinator, not a Planning Authority. If Planning Coordinator is referred to in the standard, it must be included in the Applicability section.

Response: Thank you for your comment.

Criterion 1.1 - The phrase "including nuclear generation" in Criterion 1.1 is there to define a plant site. Unit output from all units at a single plant site should be included to determine if a plant meets the 1500MW threshold. The evaluation for Critical Cyber Assets is similar. Although it is highly unlikely that nuclear and non-nuclear units share common Cyber Assets, the evaluation should still occur.

Criterion 1.3 – One of the functions identified in the Functional Model is Planning Reliability, which has an identified task of "Evaluate, develop, document, and report on resource and transmission expansion plans for the Planning Coordinator area. Integrate the respective plans, evaluate the impact of those plans on and by adjoining Planning Coordinator's integrated plans and assess whether the integrated plan meets reliability needs, and, if not, then to report on potential transmission system and resource adequacy deficiencies and suggest or facilitate the process for developing

Organization	Yes or No	Question 1 Comment
		alternative plans to mitigate identified deficiencies." The Functional Entity responsible for that function is the Planning Coordinator, who is "(t)he functional entity that coordinates, facilitates, integrates and evaluates (generally one year and beyond) transmission facility and service plans, and resource plans within a Planning Coordinator area and coordinates those plans with adjoining Planning Coordinator areas." Another function in the Functional Model is Transmission Planning, which has an identified task of "Evaluate, develop, document, and report on expansion plans for the Transmission Planner area. Assess whether the integrated plan meets reliability needs, and, if not, report on potential network conditions or configurations that do not meet performance requirements and provide potential alternative solutions to meet performance requirements." The Functional Entity responsible for that function is the Transmission Planner, who is "(t)he functional entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within a Transmission Planner area." The Reliability Coordinator, on the other hand, is "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." The focus of Criterion 1.3 is the long-term planning horizon, not real-time. Criterion 1.8 - FAC-014-2 Requirement R3 states "The Planning Authority shall establish SOLs, including IROLs, for its Planning Authority Area that are consistent with its SOL Methodology." FAC-014-2 Requirement R4 states "The Transmission Planner shall establish SOLs, including IROLs, for its Transmission Planning Area that are consistent with its Planning Authority's SOL Methodology." FAC-014-2 Requirement R1 states "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." According to FAC-014-2, the Reliability Coordinator does not develop IROLs. They ensure that the IROLs are established, and that they are consistent with their SOL methodology. Planning Authority is referenced because of FAC-014-2 Requirement R3. Also, since the Planning Coordinator would not own any Critical Assets, they are not subject to CIP-002-4 and would not be listed as a Responsible Entity.

Organization	Yes or No	Question 1 Comment
OGE	Yes	This question was answered "Yes", however the following recommendations for improvement are offered. In attachment 1, the threshold for criteria 1.1, needs to be supported by engineering principles and transmission operations knowledge. The current threshold was seemingly driven by the need to increase the number of facilities. Attachment 1, criteria 1.4, needs to be focused on the distinct units that, per the Transmission Operator's restoration plan, are used to restore the system. Units meeting the Blackstart Resource definition that are alternate or backup sources should be included in the Transmission Operator's restoration plan, but excluded from the Critical Asset criteria. Attachment 1, criteria 1.7, the response to the prior comments included the statement, "It should be noted that connections to generators or generation-only substations are not counted in this Criterion." For an effective bright-line, this needs to be supported within the standard. Reference to a supplemental document, such as the "consideration of comments", will not suffice in a compliance effort.

Response: Thank you for your comments.

Criterion 1.1 - The Standard Drafting Team performed an informal survey of the regions and identified what the megawatt value of the reserve sharing would be for various groups. The SDT used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Balancing Authorities in all regions.

Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as a Critical Asset. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage."

Criterion 1.7 – The choice of the phrases “Transmission Facilities” and “transmission stations or substations” was intentional to exclude connections

Organization	Yes or No	Question 1 Comment
for generators and generation only substations.		
Tampa Electric	Yes	We agree with the proposed language, however if this version does not pass and changes need to be made, we would strongly recommend bright line criteria for Critical Cyber Assets and a CCA identification methodology. In the absence of such criteria and associated methodology we expect inconsistency across entities, and would recommend the language here be modified as follows: "the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units via common mode failure that in aggregate exceeds Attachment 1, criterion 1.1 within 15 minutes."
Response: Thank you for your comment. The SDT will take your suggested wording under consideration for future revisions. In the absence of such criteria, please refer to the "Critical Cyber Asset Identification Guideline."		

Organization	Yes or No	Question 1 Comment
Wisconsin Electric Power Company d/b/a We Energies	Yes	We appreciate the diligence of the Standard Drafting Team in reviewing and responding to the comments and feedback provided during the previous ballot, and the changes made to the bright line criteria in Attachment 1 in response to comments and feedback. We strongly support the change to a single implementation timeline of 24 months which will simplify both implementation and audit requirements, and would like to point out the fact that there is a discrepancy in timelines specified in the draft standard and the timelines specified in the draft implementation plan. This discrepancy must be corrected in the final implementation. Also, the timeline proposed for CIP-005-4 should coincide with the timeline for the other CIP version 4 standards to further streamline compliance and audit processes. We would also like to express concern that, in so much as Criterion 1.1 could result in the identification of generation plant locations with no Critical Cyber Assets, the resulting requirements in Criterion 1.10 could result in expending efforts protecting transmission assets that might not otherwise need to be protected, diverting resources that might be more effectively expended elsewhere. Finally, we would like to express concern that the failure to specify a criticality criteria for Blackstart Resources in Criterion 1.4 will result in current blackstart-capable units not being identified as Blackstart Resources. Thank you for your consideration of these comments.
Response: Thank you for your comments. The flowchart in the implementation plan has been removed. Your comments on CIP-005-4 will be forwarded to that team. Criterion 1.10 - The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As		

Organization	Yes or No	Question 1 Comment
such, these assets deserve protection as a Critical Asset.		
Independent Electricity System Operator	No	We appreciate the Drafting Team's reinstatement of Section 4.2.1 pertaining to the exemption of facilities regulated by the CNSC. We however respectfully reiterate our objection to criteria 1.6 and 1.7. In our view, removal of some of the facilities identified as Critical Assets using these criteria will have no impact on the BES. Their inclusion on the Critical Assets list would therefore be unnecessary The Drafting Team's response to our comment was "The inclusion of a risk-based evaluation by any entity would not meet the objective of uniform application of Critical Asset identification across all entities."We must however point out that Criteria 1.3, 1.8 and 1.9 already allow entities (whether they be the RC, the PC etc.) the discretion to designate/identify as Critical Assets, facilities "necessary to avoid BES Adverse Reliability Impacts" or "critical to the derivation of IROLs". Presumably, these entities doing the "designating" will have a documented methodology and apply it. We therefore advocate a similar approach in the case of Criteria 1.6 and 1.7.We believe the list of relevant transmission facilities developed by the Responsible Entity, should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. Such an arrangement would be akin to the exemption provisions advocated by FERC in its Final Rule on Revisions to the ERO definition of Bulk Electric System.We therefore propose the following specific wording: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.1.7 Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comment. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis.		
Great River Energy	No	We believe that criterion 1.4 and 1.5 of Attachment 1 need to be revised such that they are tied more closely to criterion 1.1 and 1.3, similar to the wording contained in criterion 1.10. We feel that this is necessary due to the fact that a Blackstart Resource's main function is the restoration of critical generation assets. This would create more clarity on the classification of Blackstart Resources and cranking paths as Critical Assets. A revised criterion 1.4 could read: "Each Blackstart Resource identified in the Transmission Operator's restoration plan as being essential to the restoration of a generating unit identified in Attachment 1 criterion 1.1 or 1.3."A revised criterion 1.5 could read: "The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource identified in criterion 1.4 to the first interconnection point of the generation unit(s)...."
Response: Thank you for your comment. The SDT is unsure of your comment "We feel that this is necessary due to the fact that a Blackstart Resource's main function is the restoration of critical generation assets." A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The Blackstart Resource should not be limited to those that start other Critical Assets. A similar defense is made for criterion 1.5. Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. It was felt that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as a Critical Asset.		

Organization	Yes or No	Question 1 Comment
WECC	Yes	We believe that the proposed changes address the direction to develop a bright-line criteria to replace the individual responsible entity methodologies. This approach will lead to more uniformity and consistency across the continent in the identification of Critical Assets. While WECC continues to believe that the bright line Criteria identified in Attachment 1 of CIP-004-2 may lead to identification of fewer Critical Assets by some entities in the West than were identified using the individual methodologies required by the current version of CIP-002, we recognize the need and desire for consistency across the continent. WECC also continues to believe a similar effort in identifying a bright line criteria for Critical CYBER Assets is necessary, and encourages NERC to consider such actions in any future modification to the standard. The language "essential to the operation of the Critical Asset" is subjective and could lead to the same lack of uniformity and consistency in identifying Critical Cyber Assets that drove the changes in identification of Critical Assets. A lack of a uniform and consistent identification of Critical Cyber Assets may prevent the desired level of reliability and security.
Response: Thank you for your comment. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. In the absence of such criteria, please refer to the "Critical Cyber Asset Identification Guideline."		
Midwest ISO	No	We thank the drafting team for their efforts and the progress they have made in improving this standard since the last ballot. While we do believe the drafting team was responsive to the comments previously submitted, we believe a new issue has been identified and an existing issue persists. The standard shifts responsibility for critical asset identification to third parties. For example, criterion 1.3 essentially causes generation owners to rely on Planning Coordinators to identify their critical generators. This responsibility should not be trasnferred and Order 706 was clear that it cannot be in paragraph 328. Criterion 1.3 is ambiguous and likely will not result in any generators being identified unless the Planning Coordinator is violating the TPL standards. Adverse Reliability Impact involves impacts to the system that cause separation, cascading, instability, etc. The TPL standards require the Planning Coordinator to plan to prevent these kinds of events for multiple contingencies. Thus, this criterion should be removed.
Response: Thank you for your comment.		

Organization	Yes or No	Question 1 Comment
Criterion 1.3 - The burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.		
SPS Energy	No	While the changes in the Criteria 1.3 allow generators to be informed of whether they are designated a Critical Asset by the Planning Coordinator or Transmission Planner, that was not the point. The discretion to make such designations without proper due diligence or independent review remains. Planning studies have a wide latitude of assumptions and it would be quite easy designate one's competitor as critical and employ the assumptions in the planning models to make that happen. Lacking independence at the PC and TP level, independent review is the only way to insure competition is not blunted by this ability to designate one's competitor as critical.
Response: Thank you for your comment. Criterion 1.3 - In the Functional Model, one of the tasks of the Planning Coordinator is "Facilitates the integration of the respective plans of the Resource Planners and Transmission Planners within the Planning Coordinator area. a. Reviews the integrated plan with respect to established reliability needs considering the impact on and by adjoining systems. b. In coordination with the Resource Planners and Transmission Planners, facilitates the development of alternative solutions for plans that do not meet those reliability needs." One of the alternative solutions developed may require the availability of a particular generator to meet reliability needs and avoid an Adverse Reliability Impact Likewise, one of the tasks of the Transmission Planning function is "Evaluate, develop, document, and report on expansion plans for the Transmission Planner area. Assess whether the integrated plan meets reliability needs, and, if not, report on potential network conditions or configurations that do not meet performance requirements and provide potential alternative solutions to meet performance requirements."		

Organization	Yes or No	Question 1 Comment
Duke Energy	Yes	Yes, however we see much room for improvement and offer the following comments: o Criterion 1.2 - We previously commented that 1000 MVAR was too large, and reiterate that comment again. There are not any reactive resources that large in SERC. Is the drafting team aware of where any 1000 MVAR resources are located? o Criterion 1.3 - This criterion is less clear than before. Adding the phrase "necessary to avoid BES Adverse Reliability Impacts" potentially broadened this criterion to include every last generator on the system, because the defined term "Adverse Reliability Impact" includes tripping of generation. You need to limit this criterion to generation whose loss "could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." o Criterion 1.4 - Need to clarify that this criterion only includes the primary Blackstart Resources. Entities may include various alternative resources in their restoration plans which aren't Critical Assets, but which may not be clearly distinguished from the primary Blackstart Resources in the restoration plan. Add the phrase "that the entity intends to rely on for system restoration". o Criterion 1.7 - Wording change creates confusion as to whether generating stations are included. Insert the word "transmission" before the word "stations". o Criterion 1.8 - This criterion is less clear than before. Delete the RC, because the identification of facilities to be protected occurs in the planning timeframe. Also the unclear language "critical to the derivation of" and "their associated contingencies" should be struck. Suggested rewording: "Transmission Facilities at a single transmission station or substation location, that are identified by the Planning Authority or Transmission Planner, whose loss could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." o Criterion 1.9 - This criterion is less clear than before. Delete the RC, because the identification of facilities to be protected occurs in the planning timeframe. Also the unclear language "critical to the derivation of" and "their associated contingencies" should be struck. Suggested rewording: "Flexible AC Transmission Systems (FACTS) at a single transmission station or substation location, that are identified by the Planning Authority or Transmission Planner, whose loss could expose a widespread

Organization	Yes or No	Question 1 Comment
		area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." o Criterion 1.10 - Removing the word "directly" creates significant uncertainty regarding what scope of facilities would be included. Reinsert the word "directly", preferably after the phrase "Transmission Facilities". Also, including the word "destroyed" in the phrase "destroyed, degraded, misused or otherwise rendered unavailable" creates significant uncertainty regarding what is intended. Add the phrase "via cyber attack" after the word "unavailable". This will clarify that the evaluation only encompasses destruction, degradation or misuse that can be achieved via cyber attack, and not a physical attack on the facilities. o Criterion 1.12 - The added language is unclear. Suggested rewording: "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements whose loss could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages for failure to operate as designed." o Criterion 1.13 - As clarified on the Webinar, the language needs to be revised to clarify that the phrase "Each system or Facility" only includes discrete systems or facilities that can individually shed 300 MW or more of load. UFLS and UVLS systems are typically composed of discrete components at many locations (not interconnected), usually on the distribution system. These discrete, localized facilities would not typically interrupt 300 MW individually. o While the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities provides milestones for implementing the CIP standards, we believe that a modification is needed related to the CIP 002 milestones within this plan. The implementation plan presumes that compilation of all of CIP 002 evidence (R1. Application of Methodology; R2. Identification of the new Critical Asset; R3. Identification of the new Critical Cyber Assets; and R4. Annual Approval of the above items) occurs simultaneously for Category 1 and Category 2. This approach does not allow sufficient time for the identification of new Critical Cyber Assets (R3) and approval of the documented CCA list (R4) once new Critical Assets are identified. We believe the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities should be amended to provide a period of 6 months following identification of a new Critical Asset for the

Organization	Yes or No	Question 1 Comment
		identification of new Critical Cyber Assts associated with the new Critical Asset (R3) and the Annual Approval of the revised Critical Cyber Asset List (R4).

Response: Thank you for your comments.

Criterion 1.2 - The value of 1000 MVAR used in this criterion is a value deemed reasonable for the purpose of determining criticality. The survey that NERC conducted earlier this year showed that there were facilities that would qualify at this threshold.

Criterion 1.3 – Adverse Reliability Impact is defined as "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." The Guidance document has been modified to provide additional clarification on this issue.

Criterion 1.4 - The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. The phrase "that the entity intends to rely on for system restoration" was discussed by the SDT, but it was determined that it added no additional clarity.

Criterion 1.7 - The choice of the phrases "Transmission Facilities" and "transmission stations or substations" was intentional to exclude connections to generators and generation only substations.

Criterion 1.8 - According to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion. The wording for criterion 1.8 came from FAC-014-2 Requirement R5.

Criterion 1.9 - According to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion. The wording for criterion 1.8 came from FAC-014-2 Requirement R5.

Criterion 1.10 - Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion. The SDT discussed your suggested

Organization	Yes or No	Question 1 Comment
		changes, and determined the existing language is adequate. The term "destroyed" is listed in the definition of Critical Asset. Criterion 1.12 - The SDT appreciates the suggestion, but believes the posted wording is adequate. Criterion 1.13 - The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. Implementation Plan – Thank you for raising this concern. The SDT will review the implementation plan in the next version and revise as necessary.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments on Successive Ballot for Cyber Security 706 – CIP Version 4 Standards

Summary Consideration: A successive ballot of the Cyber Security 706 CIP Version 4 standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. The following summary of comments and responses is grouped by areas of CIP-002-4.

General Comments:

Concern was expressed that any clarification included in the Guidance Document should be made part of the Standard. The SDT responded that, while the Guidance Documents are not the standard, they do provide additional context. Other entities expressed concern that the bright line prescribed in Attachment 1 will still include smaller Registered Entities that do not have significant impact on the reliable operation of the BES. The SDT responded that in FERC Order 706, the Commission addressed the importance of Critical Assets, no matter how small. Another entity stated that there needs to be a clear and consistent method for Planning to identify IROLs, or it becomes subjective and open to interpretation. The SDT responded that the purpose of FAC-014-2 Requirements R3 and R4 is to establish a clear and consistent method for identifying IROLs. The method for Planning to identify IROLs is beyond the scope of the CIP standards. Several entities expressed an interest that the SDT should take steps to reduce ambiguous language. (e.g. black start resources). The SDT responded that they have made efforts to reduce any ambiguous language, to the point of using the NERC glossary term “Blackstart Resources” in order to eliminate any confusion over the term. Another entity expressed that criteria for critical assets should be based on critical functions of assets like system restoration, voltage control, maintaining load/generation balance, maintaining flows within IROL/SOL, critical SPS and that the list the list should not rely on substation voltages or amount of MW. The SDT responded that voltage levels and MW thresholds were used in criteria that had no corresponding bright lines in existing standards.

Several entities stated that the SDT should clarify that substations are the facilities to be identified as Transmission Critical Assets, not lines, transformers, reactive equipment, etc. The SDT responded that substations are not the only Facilities identified as Critical Assets. Lines, transformers, reactive equipment, and other Facilities can be classified as a Critical Asset if they meet any of the criteria in Attachment 1. The SDT referred commenters to the posted guidance document for additional clarification. One entity expressed concern that many items give one entity the power to designate facilities owned by another entity as critical. The SDT responded that the issue of communication

between entities is recognized as an issue that needs to be addressed and will be considered in a future version. Some entities felt that the SDT was prescriptive in determining Critical Assets, which they felt was contrary to FERC Order 706. The SDT responded that the Attachment 1 criteria were developed in response to an external oversight directive in the FERC Order 706. In consideration of this directive, the SDT decided there did not exist across all regions an appropriate third party to provide this type of oversight. Also, external review and oversight carries with it the compliance overhead and arbitration processes analogous to the TFE process. This "bright-line" criteria approach removes the variability of entity defined methodologies that would prompt the need for external review. Additionally, some entities expressed concern that the SDT should begin a similar effort in identifying a bright line criteria for Critical Cyber Assets. The SDT responded that the scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method, not the Critical Cyber Asset Identification method.

One entity stated that they disagree with the removal of R1.2.7 from CIP-002-3. The entities should continue to have the option to add assets which they feel are appropriate. The SDT responded that originally criterion 1.16 was placed in Attachment 1 to provide Responsible Entities the flexibility to include addition items on their existing Critical Asset list that did not meet any other criterion in Attachment 1. The SDT was concerned that having additional Critical Assets without criteria opens the possibility of having the burden of proof on the Registered Entity that they have no additional Critical Assets.

Commenters pointed out a numbering format issue and an abbreviation issue in the Compliance section, and the SDT corrected the issues. Several entities recommended using different wording than "annual." The SDT responded that the term "annual" exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. Another commenter stated that FERC & NERC must attempt to provide the security needed, but in a way that balances adequate security with an entities ability to absorb the costs. The SDT and volunteer industry participants have developed appropriate Critical Asset Identification criteria which have been presented to industry through various iterations for review and feedback. In addition, the SDT has attempted to factor in this issue by limiting the scope of Critical Cyber Assets to those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

Many Canadian members of NPCC are of the opinion that in Attachment 1 of the draft CIP-002-4 standard an RC led exclusion provision should be available to allow some facilities to be exempted from the CIP standards. The SDT

believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.

Nuclear Applicability:

Several entities expressed concern about the nuclear generation exemption language for nuclear generation plants located in the United States (U.S.) along with the parenthetical text of Attachment 1 criterion stating "including nuclear generation." They expressed that this leaves the standard ambiguous and in need of clarification based on recent Nuclear Regulatory Commission (NRC) findings. The NRC and NERC have worked closely to address FERC's Order 706B concerns related to any nuclear balance of plant (BOP) systems, structures and components (SSCs) within a U.S. nuclear power plant that is not regulated by the NRC and subject to NERC CIP standards. However, the NRC letter to NERC dated November 26, 2010 clarifies its findings that "Based on the Commission's [NRC] determination, the NRC staff does not believe that there will be any SSCs in the BOP that will fall under NERC's Critical Infrastructure Protection (CIP) standards." The SDT responded that the phrase "including nuclear generation" in criterion 1.1 is there to define a plant site. Unit output from all units at a single plant site should be included to determine if a plant meets the 1500MW threshold. The evaluation for Critical Cyber Assets is similar. Although it is highly unlikely that nuclear and non-nuclear units share common Cyber Assets, the evaluation should still occur. In addition, the Applicability language has been modified in light of the NRC letter.

Requirement R1:

One commenter stated that Requirement R1 should be clarified to require the first list of identified Critical Assets to be developed prior to the effective date of the Standard. The SDT responded that in order to be compliant with CIP-002-4 on the effective date of the standard, the list must be developed by the effective date. This is clarified in the implementation plan. Another commenter believes that CIP-002-4 R1 needs to clearly state "The RE should identify a list of Critical Asset that it owns..." The SDT believes the phrase "a list of its identified Critical Assets" in R1 specifies ownership of the Critical Asset by the Responsible Entity.

Requirement R2:

One commenter stated that Requirement R2 should be clarified to require the first list of identified Critical Cyber Assets to be developed prior to the effective date of the Standard. The SDT responded that in order to be compliant

with CIP-002-4 on the effective date of the standard, the list must be developed by the effective date. This is clarified in the implementation plan.

Requirement R3:

One commenter stated that Requirement R3 should be modified to require any update of the Critical Asset or Critical Cyber Asset list to be approved. The SDT debated this issue and determined that an annual approval of each list was sufficient.

Attachment 1:

Criterion 1.1

One entity asked for clarity on the terms "a defined physical footprint" and "commonly accepted generating facility terminology." Additional clarity has been added to the Guidance document. The following sentence was added to the language explaining criterion 1.1: “Single plant location refers to a group of generating units occupying a defined physical footprint, often but not always, these units are surrounded by a common fence, have a common entry point, share common facilities such as warehouses, water plants and cooling sources, follow a similar naming convention (plant name - unit number) and fall under a common management organization.” Another commenter was concerned about communication that is necessary between various Responsible Entities to identify Critical Assets. The SDT agreed that communication between various Responsible Entities will be required to ensure that all critical Assets are identified.

Criterion 1.2

One commenter expressed that 1000 MVAR was too large, and that there are not any reactive resources that large in their region. They asked if the drafting team is aware of where any 1000 MVAR resources are located. The SDT responded that the survey that NERC conducted earlier this year showed that there were facilities that would qualify at this threshold.

Criterion 1.3

One commenter expressed that criterion 1.3 was not consistent with the goal of providing bright line requirements. This criterion requires entity to conduct a study and submit to the Reliability Coordinator, Planning Coordinator or Transmission Planner, who will then determine if a facility qualifies as critical. The SDT responded that there is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed to avoid Adverse Reliability Impacts in the long-term planning horizon. However, if the PC or TP has identified Adverse Reliability Impacts (the impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection), then any units identified that avoid this scenario must be classified as a Critical Asset. Another entity requested clarification whether this criterion is for "reliability must run" units? The SDT responded that the units identified using criterion 1.3 are not necessarily designated as "reliability must run."

One commenter stated that the Reliability Coordinator should be the entity to determine the criticality of a generation Facility, based on information it receives from the Planning Coordinator. The SDT responded that based on the functional model the Planning Coordinator or the Transmission Planner are the correct entities to perform the evaluation. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.

Criterion 1.4

The APPA CIP Task Force identified what they believed to be an unintended consequence - a Catch-22 - from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them

are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

One commenter expressed concern that the Blackstart Resources term used in Criteria 1.4 and 1.5 is in the NERC Glossary and is used in EOP-005-2. However this standard and the related definition are not approved by FERC yet. So what happens if the definition of Blackstart Resource is significantly changed after approval of this standard? The SDT responded that this concern was noted prior to the second posting and the implementation plan was revised to clarify the issue.

Another commenter suggested that NERC consider a "Black Start Tier Methodology" in which only "Primary Black Start Units" would fall under stringent compliance scrutiny and obligations, while other "Secondary Tier Units" would still be made available with required annual testing and operating specifications but be taken off the scope of NERC compliance. The SDT responded that a tiered approach to Blackstart Resources is a good idea, and the SDT suggested that a SAR be submitted by the entity outlining this approach to EOP-005-2. Other commenters suggested that a 1500MW limit be included in this criterion. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as a Critical Asset

Criterion 1.5

A few commenters suggested alternate wording for this criterion. The SDT discussed the merits of each, but ultimately decided to keep the posted wording unchanged.

Criteria 1.6 and 1.7

One commenter stated that this criterion should have another factor based on the size of the facility such that loss of the Facility would have an adverse impact on the BES. The SDT will take this suggestion under consideration for future revisions. Another commenter stated that the Generator Interconnection Facilities as defined in the NERC project http://www.nerc.com/filez/standards/Project2010-07_GOTO_Project.html, should be excluded from the Transmission Facilities. The SDT believes that the Guidance document is the appropriate place for this discussion until the Generation Interconnection Facilities are incorporated into the standards.

Another commenter believed the list of relevant transmission facilities developed by the Responsible Entity should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. Such an arrangement would be akin to the exemption provisions advocated by FERC in its Final Rule on Revisions to the ERO definition of Bulk Electric System. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis.

Criterion 1.8 and 1.9

One commenter stated that there should be some obligation that the parties that identify the Transmission Facility as critical also notify the Transmission Owner and Operator of that identification so the Transmission Owner and Operator are aware and can protect. The SDT responded that FAC-014-2 R5 contains information concerning communication of Facilities that are critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

Another commenter expressed that the Reliability Coordinator be removed from the criterion that identifies Critical Asset facilities based on Interconnection Reliability Operating Limits (IROLs). The SDT responded that according to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a

responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion.

Criterion 1.10

Several commenters stated that the phrase “directly” should be included in Criterion 1.10 which existed in the previous draft. The SDT responded that several commenters in the first posting were concerned about the use of the term “directly.” After consideration by the SDT, it was determined that the term could be removed without affecting the intent of the criterion. One commenter expressed concern that, in so much as Criterion 1.1 could result in the identification of generation plant locations with no Critical Cyber Assets, the resulting requirements in Criterion 1.10 could result in expending efforts protecting transmission assets that might not otherwise need to be protected, diverting resources that might be more effectively expended elsewhere. The SDT responded that the intent of Criterion 1.10 is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset.

Criterion 1.11

Several commenters stated that this criterion should either be removed or revised to “Transmission Facilities providing offsite power requirements as identified in the Nuclear Plant Interface Requirements.” The SDT responded that Criterion 1.11 is based on NUC-001-2 R9.2.2 “Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.” While the purpose of NUC-001-2 states “This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown,” it is a NERC reliability standard and as such helps to ensure the reliability of the Bulk Electric System.

Criterion 1.12

One commenter stated that the phrase "for failure to operate as designed" is inappropriate. Most SPS's are installed for automatic response to multi-contingency events. For an IROL to be exceeded, the multi-contingency event would need to occur at system conditions that would cause an IROL to be exceeded at the same time that the SPS failed to operate. The probability of the multi-contingency event occurring at such system conditions is very small (e.g., 1 in

50 year order of magnitude frequency), and the SPS would need to fail at that same time. The SDT responded that "Failure to operate as designed" was added to this criterion to account for human error, misconfigurations, improper change management (whether unintentional or malicious)

Criterion 1.13

Several commenters asked that the Guidance Document be modified to provide the reasoning behind the 300 MW criteria listed in criterion 1.13. The SDT responded that the posted Guidance document has been modified to add reasoning for the threshold level. Other commenters suggested alternate wording for the criterion. The SDT discussed the merits of each, but ultimately decided to keep the posted wording unchanged.

Some commenters stated that criterion 1.13 should be reworded to indicate that distributed UFLS or UVLS schemes (i.e., individual UF or UV relays operating independently in multiple substations) are not considered to be a critical asset. Collectively the UFLS or UVLS scheme may shed more than 300MW; however, due to the distributed nature of the scheme, the UFLS or UVLS schemes are not considered to be a critical asset. The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. The SDT responded that a discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. This criterion is intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes.

One commenter expressed concern that the owner of a UFLS system, Distribution Provider, is not listed in the applicability section of this Standard. The SDT does not feel it necessary at this time to include Distribution Providers in the Applicability section but may consider this in future revisions of the Standards. Distribution Providers may own certain very limited BES Cyber Assets, generally limited to UFLS and UVLS relays. However, additional functional entities (i.e. Transmission Operators) generally provide aggregate control of these relays.

Criterion 1.15

One commenter asked for clarification on the term "control generation." The SDT responded that Attachment 1 criteria refer to control centers which control generation. The guidance document provides additional clarity that "control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as

a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation)." Another commenter was concerned about confusion in both applying and auditing what are apparently two independent criteria presented together as a single criterion, and recommended separation of this criterion into two criteria. The SDT decided to group the criteria for control centers based on functionality. Separating them does not appear to add any additional clarity to the criteria.

Another entity expressed concern that if a small utility, as a joint owner, has control over only a small portion of a large plant that falls under the brightline of criterion 1.1, they are concerned that as currently written, the first sentence of criterion 1.15 would designate this small utility's control center as critical. The SDT responded that the concern is that the joint owner's control center could provide a path to compromise the functionality of the generation designated a Critical Asset.

Criteria 1.16 and 1.17

One commenter stated that they believe that in Criterion 1.16 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. The SDT responded that due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. Attachment 1 criteria are used to identify control centers as Critical Assets. The consideration of specific reliability functions would be a part of the entity identifying Critical Cyber Assets which support the control center.

Implementation Plan

One entity stated that the proposed implementation is too aggressive. Physical Security Perimeters are expensive and it may not be possible to fund these modifications in the short timeframe for compliance. A 3-year implementation period would be more appropriate. The SDT believes there is precedent showing this implementation period is reasonable. Upon FERC Approval, the Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.

Balloter	Company	Seg-ment	Vote	Comment
Kirit S. Shah	Ameren Services	1	Affirmative	1. We suggest Criteria 1.6, 1.7 and 1.10 should be changed to include substations and switchyard (station) only and not "Facilities". Based on the definition of "Facilities" and application of Criteria 1.6, 1.7 and 1.10, the Critical Asset list now would include transmission lines. Our concern is that there will be significant issue to comply with CIP-003 through CIP-009 (for example, physical security requirements) for the transmission line assets, if some components installed on the lines fall into cyber asset category, such as temperature or flow monitoring devices or fiber optics used for communication. 2. The Blackstart Resources term used in Criteria 1.4 and 1.5 is in the NERC Glossary and is used in EOP-005-2. However this standard and the related definition are not approved by FERC yet. So what happens if the definition of Blackstart Resource is significantly changed after approval of this standard? We suggest that the definition of Blackstart Resources should be included in this standard. 3. The phrase "directly" should be included in Criterion 1.10 which existed in the previous draft. We believe that after removing this term, the revised wordings now are more confusing. 4. We believe that in Criterion 1.16 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. We suggest that Criterion 1.16 should be modified to read "Each control center or backup control center used to perform the functional obligations, pertaining to real time operation of the BES, of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12." 5. We believe that in Criterion 1.17 the functional obligation should be clearly defined to include those pertaining to the real-time operations and NOT all. Further this criterion should make clear that the 1500 MW is calculated on the same basis as defined in Critetion 1.1. We suggest that Criterion 1.17 should be modified to read, "Each control center or backup control center used to perform the functional obligations, pertaining to real time operation of
Jennifer Richardson	Ameren Energy Marketing Co.	6		

Balloter	Company	Seg-ment	Vote	Comment
				the BES, of a Balancing Authority if its Balancing Authority Area(s) includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations pertaining to real time operation of the BES, of a Balancing Authority if its Balancing Authority Area(s) includes an aggregate of 1500 MW in a single Interconnection, calculated using the highest rated net Real Power capability of each unit during the preceding 12 months. 6. During the Webinar, references were made to the Guidance Document. However, the Guidance Document is NOT the standard and can not be used in the compliance audit. So, any clarification included in the Guidance Document should be made part of the Standard.

Response: Thank you for your comments.

1. The SDT does not feel this change is necessary. Please refer to the first bullet in the Overall Application of Attachment 1 in the posted Guidance document for a discussion of the SDT's reason for the use of the term "Facility."
2. Your concern was noted prior to the second posting and the implementation plan was revised with the following: "The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities." The language has been revised in this posting to "The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted to FERC for regulatory approval in the US with Project 2006-03 – System Restoration and Blackstart. The Effective Date of EOP-005-2 is the date that Criteria 1.4 and 1.5 will be used to determine Critical Assets for any Responsible Entity."
3. Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion.
4. Due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. Attachment 1 criteria are used to identify control centers as Critical Assets. The consideration of specific reliability functions would be a part of the entity identifying Critical Cyber Assets which support the control center.
5. Due to the direct impact on the operation of identified Critical Assets, these Balancing Authority control centers must be designated as Critical Assets. The impact to the identified Critical Assets would be in real time, as the Balancing Authority functions in the Functional Model involve real time operations. If a Balancing Authority can control 1500MW or more of generation, it is considered a Critical Asset. The language in criterion 1.1 was taken from MOD-024, which is only applicable to Generation Owners.
6. While the Guidance Documents are not the standard, they do provide additional context. The SDT believes the wording in the posted standard provide sufficient clarity.

Balloter	Company	Seg-ment	Vote	Comment
Paul B. Johnson	American Electric Power	1	Affirmative	While not all of the concerns AEP raised in the last comment period were addressed, AEP can support this draft moving forward.
Edward P. Cox	AEP Marketing	6		
Brock Ondayko	AEP Service Corp.	5		
Response: Thank you for your comments.				
Jason Shaver	American Transmission Company, LLC	1	Affirmative	ATC supports Version 4 of the CIP Standard,however, believes that Attachment 1, the so-called bright line criteria, language needs to be clarified. There needs to be a clear and consistent method for Planning to identify IROLs, or it becomes subjective and open to interpretation. Please refer to ATC's recommended changes to the Criteria in their submitted comments for the NERC project.
Response: Thank you for your comments. The purpose of FAC-014-2 Requirements R3 and R4 is to establish a clear and consistent method for identifying IROLs. The method for Planning to identify IROLs is beyond the scope of the CIP standards.				
Gregory S Miller	Baltimore Gas & Electric Company	1	Affirmative	BGE thanks the SDT for their positive response to the previously submitted comments. BGE asks that the SDT consider adding to the Guidance Document the reasoning behind the 300 MW criteria listed in the automatic load shedding criteria 1.13 in Appendix 1.
Response: Thank you for your comments. The posted Guidance document has been modified to add reasoning for the threshold level.				
Gordon Rawlings	BC Transmission Corporation	1	Negative	BC Hydro agrees with the controls suggested around remote access but some clarification is required R6 - This is pretty wide open. Suggest that specific requirements be put forth so entities know exactly what they need to comply with. Instead of providing “examples” or “includes”, explicitly define those items that constitute support and maintenance. R6.4.2 – Recommends the use of SIEM technology to “alert” on access attempts by unauthorized parties. This automates the monitoring but would need clarification that this satisfies this requirement. R6.5 - Such a user agreement does make these users aware of their respective responsibilities in

Balloter	Company	Seg-ment	Vote	Comment
				ensuring the security of the CCA in question. However, this is a weak control as an entity cannot influence direct control over how these entities implement security (i.e. Areva desktops) on their computer devices used to support entities CCAs. Does having such a signed agreement in place satisfy compliance? Can these agreements be entered into with organizations (i.e. Areva) as security policies are typically enforced uniformly throughout organizations?
Response: Thank you for your comments. Your comments will be passed on to the Project 2010-15 drafting team.				
Donald S. Watkins	Bonneville Power Administration	1	Negative	BPA believes that the bright line criteria approach in CIP-002-4 is an improvement over prior versions. However, it still does not address the concern by the industry in regards to providing sufficient clarity to many portions of CIP-002-4 to make it acceptable to the majority of utilities that must understand and develop strategies to meet the standards and requirements and implement them in a reasonably timely fashion. BPA still supports the formal comments that we submitted in October 2010. Additional comments: CIP-002-4 R2.1. “The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter” does not go far enough in its definition of what qualifies as a critical cyber asset and needs further clarification, particularly concerning serial devices. For example: What exactly is meant by "uses a routable protocol to communicate outside the Electronic Security Perimeter"? 1. Can a device that is not capable of native routable protocol (does not have, or use an ethernet card) qualify as using routable protocol? 2. Does a device that is not capable of native routable protocol, that is connected to a device which is ethernet connection outside the ESP (Serial to Ethernet Converter) qualify? 3. Does a device that is not capable of native routable protocol, but is connected to a Terminal Server, which is ethernet connected outside the ESP qualify? 4. Does it make a difference if there is only view access to the internal ESP device with no
Rebecca Berdahl	Bonneville Power Administration	3		
Francis J. Halpin	Bonneville Power Administration	5		

Balloter	Company	Seg-ment	Vote	Comment
Brenda S. Anderson	Bonneville Power Administration	6		possible ability to control it? 5. What if the device is connected to another device which is ethernet connected, but it simply dumps to a data-store on that device, and there is no access through to the data-store device (the internal ESP device)? 6. What if the device itself never initiates communications outbound, and can only be connected to if access is initiated to it from elsewhere? 7. What if the device has no ability to connect to and influence any other device? 8. What if you can't connect to that device and through it connect to any other device? 9. What if the Serial to Ethernet device between the Cyber Asset and the network strips all routable protocol information off and forwards only non-routable data to the Cyber Asset.
Response: Thank you for your comments. Requirement R2: This language has existed in versions 1 through 3 of CIP-002. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Also, please refer to the "Identifying Critical Cyber Assets" document for additional clarification.				
Melissa Kurtz	U.S. Army Corps of Engineers	5	Negative	-- The bright line criteria for identification of Critical Assets takes away the flexibility of entities to define what their Critical Assets are --The latest revision to Attachment 1 no longer includes an item indicating that the Responsible Entity may include any additional assets that the Responsible Entity deems appropriate to include. --CIP-002-4 R2.1. "The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter" does not go far enough in its definition of what qualifies as a critical cyber asset and needs further clarification, particularly concerning serial devices. For example: What exactly is meant by "uses a routable protocol to communicate outside the Electronic Security Perimeter"? 1. Can a device that is not capable of native routable protocol (does not have, or use an ethernet card) qualify as using routable protocol? 2. Does a device that is not capable of native routable protocol, that is connected to a device which is ethernet connection outside the ESP (Serial to Ethernet Converter) qualify? 3. Does a device that is not capable of native routable protocol, but is connected to a Terminal Server, which is ethernet connected outside the ESP qualify? 4. Does it make a difference if there is only view access to the internal ESP device with no possible ability to control it? 5. What if the device is connected to another device which is ethernet connected, but it simply dumps to a data-store on that device, and there is no access

Balloter	Company	Seg-ment	Vote	Comment
				through to the data-store device (the internal ESP device)? 6. What if the device itself never initiates communications outbound, and can only be connected to if access is initiated to it from elsewhere? 7. What if the device has no ability to connect to and influence any other device? 8. What if you can't connect to that device and through it connect to any other device? 9. What if the Serial to Ethernet device between the Cyber Asset and the network strips all routable protocol information off and forwards only non-routable data to the Cyber Asset.
Response: Thank you for your comments. Requirement R2: This language has existed in versions 1 through 3 of CIP-002. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Also, please refer to the "Identifying Critical Cyber Assets" document for additional clarification.				
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	Brazos Electric appreciates the work of the SDT and is supportive of the efforts and the general concepts of this draft. This is a negative vote due to disagreement over some elements in Attachment 1 criterion. See comments separately submitted.
Response: Thank you for your comments. Please refer to the response to comment document.				
Paul Rocha	CenterPoint Energy	1	Negative	CenterPoint Energy was extremely disappointed in this latest effort from the SDT and cannot support the proposed Standard in its current form. While the SDT did revise some criteria in Attachment 1 in response to industry comments, CenterPoint Energy believes the latest proposed Standard is less palatable than the previous version. Specific CenterPoint Energy concerns are as follows. The SDT's response to comments on Criterion 1.4 would seem to indicate a belief that the industry does not understand the term "Blackstart Resource". To the contrary, CenterPoint Energy believes the SDT fails to understand the contents of restoration plans and the far reaching implications of this criterion as pointed out by multiple comments.

Balloter	Company	Seg-ment	Vote	Comment
				CenterPoint Energy believes the revisions made to Criterion 1.5 do not adequately address commenter's concerns and, in fact, adds ambiguity to the Standard. The SDT did not address concerns regarding the phrase "initial switching requirements". In addition, the moving of the phrase, "…as identified in the Transmission Operator's restoration plan" to the end of the criterion potentially adds a requirement to the restoration plan where none currently exists. In Criterion 1.10, comments were made asking for clarity for the term "directly connected". Instead of providing the requested clarity the SDT chose to delete the word "directly" resulting in an even more ambiguous criterion. CenterPoint Energy is particularly concerned that the SDT chose to dismiss comments regarding Criterion 1.11. The SDT appears to have based its decision on a false understanding of the purpose of NUC-001-2. In its response, the SDT stated; "Since these facilities were deemed so important that a NERC reliability standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets." Using the SDT's logic, any BES facility or practice addressed by a NERC Standard would be deemed "critical" to BES reliability. Moreover, the Purpose section of NUC-001-2 clearly states that the Standard was developed to require "…coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown." In addition, as previously pointed out by CenterPoint Energy, as per NUC-001-2 R2, NPIR's are developed by a negotiated methodology between the NPGO and the Transmission Entity. As a result the facilities essential to meeting the NPIR's are also a result of a negotiated methodology, therefore each situation could have an entirely different set of NPIR's and associated facilities. CenterPoint Energy fails to see this as a "bright line" criterion. CenterPoint Energy strongly disagrees with the SDT's revisions to Criterion 1.13. In its response to comments, the SDT gives no indication any comments indicated a need to include UFLS and UVLS in this criterion. In fact, the SDT stated that several commenters indicated a need to clarify that this criterion applied to a single common control system only. Instead of addressing this concern, the SDT chose to go in a different direction as it completely changed the criterion from pertaining to a common control system to one that could possibly be applicable to distributed

Balloter	Company	Seg-ment	Vote	Comment
				load shedding devices on an entity's distribution system. The SDT's statement "This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes" demonstrates a clear lack of understanding of UFLS and UVLS load shedding schemes as they are applied throughout the industry. In summary, CenterPoint Energy believes that the SDT has demonstrated a lack of understanding of industry practices and is unwilling or unable to adequately address industry concerns. Members of the SDT should represent industry stakeholders and produce Standards the industry can support. However, SDT's are not voted into position by industry stakeholders and therefore are not accountable to the industry, as evidenced by the unresponsive nature of this SDT. If the revised Standard is again rejected by the industry, CenterPoint Energy recommends the current SDT be disbanded and a new SDT be seated in order to complete this project in a reasonable fashion that addresses industry concerns and meets Commission directives. CenterPoint Energy believes there is value to retaining SDT members who dissented from the majority opinion of the SDT, and supports a process to allow such existing SDT members who dissented from the majority opinion to apply for the new SDT if CenterPoint Energy's proposal is accepted.

Response: Thank you for your comments.

Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.

Criterion 1.5 – EOP-005-2 Requirement R1.5 states "Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started." This is already an element of the Transmission Operator's restoration plan.

Criterion 1.10 - Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion.

Criterion 1.11 - Criterion 1.11 is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." While the purpose of NUC-001-2 states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown," it is a NERC reliability standard and as such helps to ensure

Balloter	Company	Seg-ment	Vote	Comment
the reliability of the Bulk Electric System. Criterion 1.13 - During the previous ballot and comment period, the SDT received many comments on this criterion. Some commenters stated that the previous wording of this criterion would inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. This criterion was intended by the SDT to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. The SDT is appointed by the Standards Committee, the process of which is outside the scope of Project 2008-06.				
David Batz	Edison Electric Institute	1	Abstain	EEI supports approval of this draft of CIP-002-4. We are concerned about ambiguous language that could lead to confusion or be open to interpretation. We recommend that the Standards drafting team consider suggestions to add clarity, particularly regarding the scope of black start facilities that will be subject to designation as Critical Assets.
Response: Thank you for your comment. The SDT has made every effort to reduce any ambiguous language. In your example the SDT chose the NERC glossary term "Blackstart Resources" in order to eliminate any confusion over the term.				
Ajay Garg	Hydro One Networks, Inc.	1	Negative	Hydro One restates its position and maintains its negative vote for the following reasons: 1. We do not believe the standard will result in an improvement in reliability since the revisions merely replace the risk-based assessment methodology in the current version with a list of criteria that will ultimately result in inclusion of facilities on the Critical Assets list that are non-impactive on the reliability of the BES. 2. We do not agree with criteria 1.6 and 1.7 in Attachment 1 as written. Application of these criteria would result in the inclusion of facilities that will have no impact on the BES reliability. We believe that the list of applicable facilities should be determined following an impact-based assessment to be performed by the Reliability Coordinator or the Planning Coordinator. If necessary, an additional requirement that requires the RC or PC to have a risk-based assessment

Balloter	Company	Seg-ment	Vote	Comment
David L Kiguel	Hydro One Networks, Inc.	3		methodology and to conduct/review the assessment should be included. We therefore propose the following wording to replace 1.6 and 1.7 in Attachment 1: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the RC (or the PC) determines that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission Facilities operated at 300 kV, at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations, unless the annual review performed by the RC (or the PC) determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages. 3. We do not believe the SDT addressed our comments submitted with the previous ballot.
Response: Thank you for your comments. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis. In addition, the SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight.				
Bernard Pelletier	Hydro-Quebec TransEnergie	1	Negative	1.3 Each generation Facility that the Planning Coordinator or Transmission Planner or the RC designates and informs the Generator Owner as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon. 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages. 1.7 Transmission Facilities operated at 300 kV or higher interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the RC determines that destruction, degradation or unavailability of those assets will not have impact outside the local area and will not cause BES instability, separation, or cascading outages. Also, we believe that to be an effort to "cast a wider net" and capture more assets without qualifying their actual criticality.

Balloter	Company	Seg-ment	Vote	Comment
				Attachment 1 inclusion criteria for critical assets should be based on critical functions of assets like: system restoration, voltage control, maintaining load/generation balance, maintaining flows within IROL/SOL, critical SPS. This list should not rely on substation voltages or amount of MW.
Response: Thank you for your comments. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis. In addition, the SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Voltage levels and MW thresholds were used in criteria that had no corresponding bright lines in existing standards.				
Michael Gammon	Kansas City Power & Light Co.	1	Affirmative	The proposed bright line is not clear for some of the bright line items. Items that are not clear introduces uncertainty and promotes interpretation issues and debates. The current proposal does not go far enough to exclude the facilities of smaller entities that do not have a significant impact on the reliability of the bulk electric system.
Charles Locke	Kansas City Power & Light Co.	3		
Jessica L Klinghoffer	Kansas City Power & Light Co.	6		

Balloter	Company	Seg-ment	Vote	Comment
Response: Thank you for your comment. The SDT has made effort to reduce any ambiguous language. Bright line criteria by its very nature may overreach in some areas and under-reach in others, with the end result being a more protected system on average.				
John W Delucca	Lee County Electric Cooperative	1	Negative	Compliance Monitoring Process Section D paragraph 1.1.2 of the CIP2v4 standard seeks to identify exceptions to the RE acting as the CEA but then lists as an exception an example where the RE DOES serve as the CEA. The intent of 1.1.2.1 is unclear. 1.1.2 The RE Shall serve as the CEA with the following exceptions: 1.1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority. Attachment 1 & Criteria Suggestions Attachment 1: • Paragraph 1.13 was modified from the previous CIP2v4 draft with the objective of clarifying the intent of the SDT to address Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program. This modification in addition to the deletion of the "common control system" terminology resulted in confusion surrounding the applicability of the 1.13 criteria to discrete relays whose sum may exceed 300MW. During the NERC Webinar on December 6, 2010, Howard Gugel clarified that the intent of the 1.13 criteria was NOT to include these discrete relays. To prevent any confusion when auditing to this standard, the intent should be clear within the standard itself and reinforced by supporting guideline documents. Suggested change to Attachment 1 paragraph 1.13: Each common control system or Facility that performs automatic load shedding, without human operator initiation, of 300MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program. Alternate Suggested change to Attachment 1 paragraph 1.13: Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program. This criterion is not intended to include systems where the 300 MW

Balloter	Company	Seg-ment	Vote	Comment
				or more threshold is met by an aggregate of discrete UF relayed distribution circuits.
Response: Thank you for your comments. The Compliance Monitoring Process language has been developed by NERC legal staff for use in all standards being developed. Criterion 1.13 - A discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. During the previous ballot and comment period, the SDT received many comments on this criterion. Some commenters stated that the previous wording of this criterion would inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. This criterion was intended by the SDT to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. The SDT appreciates the suggested wording, but believes the posted wording is adequate.				
Martyn Turner	Lower Colorado River Authority	1	Affirmative	For CIP-002-4 Attachment 1, item 1.13 it should modified to read as follows to better clarify the system referred to in the item: 1.13. Each Protection System or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.
Response: Thank you for your comments. The SDT appreciates the suggested wording, but believes the posted wording is adequate.				

Balloter	Company	Seg-ment	Vote	Comment
Joe D Petaski	Manitoba Hydro	1	Negative	-We disagree with the removal of R1.2.7 from CIP-002-3. The entities should continue to have the option to add assets which they feel are appropriate. There is no obligation within the language of the standard which requires an entity to identify additional assets. An entity should not be found non-compliant for identifying Critical Assets outside of the Attachment 1 criteria, and should not be found non-compliant for not identifying any additional assets. -It is unclear if the 300MW is shed simultaneously or in blocks over time. The loss of generation or the loss of load are analogous in their reliability impact on the BES, thus criterion 1.13 using a 300 MW threshold seems inconsistent with criterion 1.1 using a 1500 MW threshold. -The thresholds appear arbitrary. No rationale has been provided for their selection. -The 15-minute "real-time" criterion should be applied to all Critical Cyber Assets, not just generation cyber assets. Implementation Plan Comments: Implementation Plan for Version 4 of Cyber Security Standards -Under the Prerequisite Approval section, the statement "The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities" only applies to entities under FERC jurisdiction. The terms are approved by the NERC BOT, and are therefore in effect for entities not under FERC jurisdiction, such as Canadian entities. Implementation Plan for Newly identified Critical Cyber Assets and Newly Registered Entities – The proposed 18 month timeframe is too short for the industry to meet compliance for a group of new CCAs. Although the existing approved Implementation Plan for Newly
Greg C. Parent	Manitoba Hydro	3		
S N Fernando	Manitoba Hydro	5		

Balloter	Company	Seg-ment	Vote	Comment
Daniel Prowse	Manitoba Hydro	6		Identified Critical Cyber Assets and Newly Registered Entities provides up to 18 months to reach compliance for some requirements under an existing program, the identification of new CCAs would distributed over time, both throughout the entity and throughout the industry. This new CIP-002-4 compliance date could cause a sudden increase in the number of new CCAs throughout the industry, which may not have the resources to meet this sudden compliance burden. Some consideration should be given to the types of environments and their unique challenges when establishing compliance dates.

Response: Thank you for your comments

Originally criterion 1.16 was placed in Attachment 1 to provide Responsible Entities the flexibility to include addition items on their existing Critical Asset list that did not meet any other criterion in Attachment 1. Many commenters stated that this was contrary to providing a bright line for Critical Asset identification, with which the SDT agrees. In addition, it has the potential of causing issues in compliance audits. The SDT was concerned that having additional Critical Assets without criteria opens the possibility of having the burden of proof on the Registered Entity that they have no additional Critical Assets. The NERC compliance and auditing process does not prohibit an entity from applying the requirements of CIP-003 to CIP-009 to any Cyber Assets.

A single discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. It is a sum of all of the blocks of load that can be shed by a single discrete component.

The posted Guidance document has been modified to add reasoning for the threshold level. The SDT and volunteer industry participants have expended considerable effort to develop consistent Critical Asset Identification approaches. The team endeavored to include work already required by other standards, and provide some constraints for an entity's assessment. These approaches, in their various iterations, have been presented to industry for review and comment. The industry provided significant feedback for the need to simplify the Critical Asset identification approach. The Attachment 1 criteria were under development for CIP-010 when the team was asked to use the criteria for the basis of a new CIP Version 4 set of standards. The results of the recent NERC data request were used to assist the team in developing the criteria in Attachment 1.

The 15-minute threshold is intended to include only those assets at generating units affecting real-time operations. This qualifier is particularly important to a generating plant because several systems (i.e. a fuel-handling system) may be essential after a longer period of time but do not necessarily involve real-time reliability impact.

The Implementation Plan for Version 4 has been modified to clarify that the Effective Date of EOP-005-2 is the date that criteria 1.4 and 1.5 will be used to determine Critical Assets for any Responsible Entity.

The Effective Date was updated prior to the ballot posting for CIP-002-4 through CIP-009-4 to "The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)." The SDT believes there is precedent showing this implementation period is reasonable. The Responsible Entity has a minimum of 2 years to become compliant with new Critical Cyber Assets. This period is consistent with

Balloter	Company	Seg-ment	Vote	Comment
the implementation plan for version 1 of the CIP Cyber Security Standards and the implementation plan for Registered Entities identifying their first Critical Cyber Asset.				
Randi Woodward	Minnesota Power, Inc.	1	Negative	Minnesota Power believes that CIP-002-4 R1 needs to clearly state "The RE should identify a list of Critical Asset that it owns…" While the Standard Drafting Team did speak to this in its response to the California ISO's comments, the SDT did not go far enough to eliminate potential interpretation issues in the future. Specifically, there is ambiguity as to what this would mean from a Balancing Authority perspective. The "its assets" language as written could be interpreted to mean the assets it controls, rather than those assets it owns. As such, we would urge the Standard Drafting Team to reconsider, and include a stronger ownership statement in the proposed Standard language.
Response: Thank you for your comment. The drafting team believes the phrase "a list of its identified Critical Assets" in R1 specifies ownership of the Critical Asset by the Responsible Entity.				
Richard Burt	Minnkota Power Coop. Inc.	1	Negative	See comments submitted by NSRS
Response: Thank you for your comments.				
James McMorran	Nevada Power Co.	1	Negative	This draft requires more work before it is affirmed. Specifically it does not define the term, "Control Generation". The standard needs to be clear whether this means the control rooms that house the distributed control systems, turbine controls, boiler controls, etc., or the facilities that provide loading instructions (which in some cases could be a Merchant function), or the traditional grid control center that may have AGC functions and issue reactive power instructions to the generating plant. Editing is required to exclude black start units in systems that are inconsequential to the Interconnection. We assume entities should not be required to declare that generator, cranking path AND its control center all to be Critical Assets if they are inconsequential to the Interconnection. We disagree with the idea that all black start units are Critical Infrastructure no matter what the impact on the Interconnection is. Some are not Critical Infrastructure.
Response: Thank you for your comments. Attachment 1 criteria refer to control centers which control generation. The guidance document provides additional clarity that "control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation)."				

Balloter	Company	Seg-ment	Vote	Comment
The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				
Rich Salgo	Sierra Pacific Power Co.	1	Negative	While the drafting team has done a commendable job on the latest draft, there remain several provisions that cause this "negative" vote: The language in the Attachment 1 concerning control centers now links the inclusion of a control center if it in any way controls a black start generator. We believe that this over-reaches and may include control centers or control rooms that would otherwise have no consequence to the reliability of the BES. There is lack of specificity about what it means to "control generation". It is still unclear whether this means the control rooms that house the distributed control sytems, turbine controls, boiler controls, etc., or the facilities that provide loading instructions (which in some cases could be a Merchant function), or the traditional grid control center that has AGC functions and issues reactive power instructions to the generating plant. We still maintain that not all black start units that are mentioned in a TOP's restoration plan rise to the level of "Critical". Perhaps only the primary black start resource should be included. This is a disincentive for entities to establish multiple (and hence, more reliable) means to black start their systems.
Response: Thank you for your comments. Attachment 1 criteria refer to control centers which control generation. The guidance document provides additional clarity that "control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation)." The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. The SDT considered using the word “primary”, but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2.				
Frank F. Afranji	Portland General Electric Co.	1	Affirmative	PGE will submit comments through the separate simultaneous comment opportunity.
Response: Thank you for your comment.				
Brenda L	PPL Electric	1	Affirmative	PPL Electric Utilities Corporation (“PPL EU”) has separately submitted comments.

Balloter	Company	Seg-ment	Vote	Comment
Truhe	Utilities Corp.			
Response: Thank you for your comment.				
Pawel Krupa	Seattle City Light	1	Affirmative	Seattle City Light supports the Standard Drafting Team's proposed changes for the successive ballot of CIP-002-4 because it provides greater precision to the identification of those Critical Assets essential to the reliability to the bulk power system. Seattle City Light commends the changes made in the successive ballot text of Appendix A to address City Light's previous comments about Critical Asset Criteria 1.13 and 1.15. Nevertheless, the revised proposed Standard continues to contain imperfections with the language that may frustrate its promise of bringing greater certainty and consistency. Imprecise language has been a recurring problem all throughout the short life of the NERC Mandatory Reliability Standards. Unnecessary compliance difficulties, tortured interpretations, and wasteful efforts have resulted. Lack of care with language threatens the existing regulatory regime by fostering distrust among industry, regulators, government, and the public at large. As such, Seattle City Light provides the following comments in the hope that the language yet will be clarified: 1. Requirement 2 of proposed CIP-002-4 states, "For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1." As previously commented, Seattle City Light finds the term 'shared Cyber Assets' unclear and suggests clarification as follows:
Dana Wheelock	Seattle City Light	3		

Balloter	Company	Seg-ment	Vote	Comment
Hao Li	Seattle City Light	4		"For each group of generating units (including Nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets networked to a system that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1." 2. Section D, Item 1, is numbered "1.1 Compliance Enforcement Authority, 1.2 The RE shall…, 1.3 Compliance Monitoring and Enforcement Process, 1.4 Data Retention, and 1.5 Additional Compliance Information." Seattle City Light believes existing point 1.2 is intended to be subordinate to point 1.1, and thus should be renumbered 1.1.1, and the remainder of points renumbered as appropriate. This change will result in further renumbering to the subpoints now listed under 1.2 as 1.2.1, 1.2.2, etc, but Seattle City Light is not certain if these subpoints should be subordinate to new 1.1.1 or if they should be equal to new 1.1.1. 3. Critical Asset criterion 1.7 of CIP-002-4, Appendix A, identifies as Critical Assets "Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations." As previously commented, Seattle City Light believes additional detail is needed about the nature of the specified interconnections. In particular, questions exist as to type (what about a radial line connected to a generator—does it count?) and distance (does a high-voltage bus count if connected to another substation a dozen feet away?). 4. Critical Asset criterion 1.13, as revised for the successive ballot, now identities as Critical Assets "Each system or Facility that performs automatic load shedding, without human operator intervention, of 300 MW or more implementing Under Voltage Load Shedding ((UVLS) or Under Frequency Load Shedding (UFLS)) as required by the regional load shedding program." Seattle City Light appreciates the clarification to exclude non-material SCADA systems from this criterion but it is not certain what precisely the Standard Drafting Team means by the revised text beginning with "…implementing Under Voltage…" and recommends clarification.
Michael J. Haynes	Seattle City Light	5		

Balloter	Company	Seg-ment	Vote	Comment
				5. Critical Asset criterion 1.15 states "Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each Control Center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection." Seattle City Light is concerned about confusion in both applying and auditing what properly are two independent criteria presented together as a single criterion. Seattle City Light recommends separation of this criterion into two criteria, as follows: "1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4." and "1.18. Each Control Center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection." 6. Critical Asset criterion 1.1.7 states "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than the aggregate of 1500 MW in a single Interconnection." Seattle City Light is concerned about confusion in both applying and auditing what properly are two independent criteria presented together as a single criterion. Seattle City Light recommends separation of this criterion into two criteria, as follows: "1.17. "Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13." and "1.19. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than the aggregate of 1500 MW in a single Interconnection."
Response: Thank you for your comments. 1. The SDT appreciates the suggestion, but believes the posted wording is sufficient. 2. The SDT agrees and has incorporated the change. 3. The SDT believes there is sufficient detail about this in the posted Guidance document. 4. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and				

Balloter	Company	Seg-ment	Vote	Comment
targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. 5. The SDT decided to group the criteria for control centers based on functionality. Separating them does not appear to add any additional clarity to the criteria. 6. The SDT decided to group the criteria for control centers based on functionality. Separating them does not appear to add any additional clarity to the criteria.				
Horace Stephen Williamson	Southern Company Services, Inc.	1	Affirmative	Southern believes that the SDT's changes to the proposed standard were responsive to some of the feedback received; however, certain key industry comments still have not been adequately addressed. For example, in Attachment 1, Section 1.11 should be deleted. Section 1.11 relates to Transmission Facilities necessary to secure offsite power to permit safe reactor shutdown. Although such Transmission Facilities are within the scope of Nuclear Plant Interface Coordination standards (NUC reliability standards), they are not within the intended scope of the Cyber Security standards (CIP reliability standards). The Purpose section of the NUC reliability standards states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown." The Purpose section of the CIP reliability standards states "NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System." Therefore, Section 1.11 should be deleted because it is clearly out of scope. Moreover, the criticality of facilities for BES reliability purposes should not be based on fuel type alone. In addition, Southern believes the following proposed changes made by the SDT should be reconsidered: In Attachment 1, Section 1.10, the SDT deleted the word "directly" by changing "generation interconnection required to directly connect generator output" to "generation interconnection required to connect generator output." The word "directly" should not be deleted from Section 1.10 because it is necessary to appropriately define the scope of the requirement. Removing the word "directly"
Richard J. Mandes	Alabama Power Company	3		
Anthony L Wilson	Georgia Power Company	3		
Don Horsley	Mississippi Power	3		

Balloter	Company	Seg-ment	Vote	Comment
				removes the bright line criteria, which is the goal of the new standard. As proposed by the SDT, the standard would require various risk-based analyses i.e. load flow and transient stability studies to determine the assets in scope. Therefore, the SDT should reconsider this proposed change. The proposed Section 1.13 would be clearer if it were changed to the following: "1.13. Each system or facility that implements Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) of 300 MW or more without human operator initiation as required by the regional load shedding program."
Response: Thank you for your comments. Criterion 1.11 – This criterion is based on NUC-001-2 R9.2.2 "Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs." Since these facilities were deemed so important that a NERC reliability standard was written and adopted to clarify the issue, the SDT determined that this was adequate justification to include them as Critical Assets. While the purpose of NUC-001-2 states "This standard requires coordination between Nuclear Plant Generator Operators and Transmission Entities for the purpose of ensuring nuclear plant safe operation and shutdown," it is a NERC reliability standard and as such helps to ensure the reliability of the Bulk Electric System. Criterion 1.10 - Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion. Criterion 1.13 - The SDT appreciates the suggestion, but believes the posted wording is adequate.				
James L. Jones	Southwest Transmission Cooperative, Inc.	1	Affirmative	The current draft of CIP 2-4 as a definite improvement over the existing CIP 2-3. It comes down to whether the failure to approve CIP-004-2 will ultimately result in more onerous CIP requirements in the future.
Response: Thank you for your comment.				
John Tolo	Tucson Electric Power Co.	1	Negative	We feel that the CIP-002-4 is overly prescriptive and does not provide a technical justification for moving away from the Reliability Based Risk Assessment Methodology(RBAM). Our opinion is the the current RBAM is a logical, reasonable, and reliable way to determine critical assets rather than a more arbitrary, "bright line" threshold contained in the proposed Requirements.

Balloter	Company	Seg-ment	Vote	Comment
				We have no issues with the changes to the other Version 4 CIP Standards regarding Nuclear facilities.
Response: Thank you for your comment. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method.				
Brandy A Dunn	Western Area Power Administration	1	Negative	With regard to identifying Critical Assets, Attachment 1 of the proposed CIP-002-4 standard is a step forward because it removes much of the ambiguity which existed under the three previous versions of the CIP standards. However, with regard to identifying Critical Cyber Assets, the proposed CIP-002-4 standard is a step backward because it increases ambiguity. It will lead to more rather than less confusion as to what is, and what is not, a Critical Cyber Asset. The "WECC Position Paper for the ballot of Project 2008-6" states, "...the failure to provide similar bright line criteria for identifying Critical Cyber Assets makes the current version unacceptable." The situation is actually worse than what the WECC states. Not only does the proposed standard fail to provide bright line criteria for identifying Critical Cyber Assets, it removes the following lanuage which existed in previous versions of the CIP standards: "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange." The language which was removed, is the language which UGP relied on when developing its Critical Cyber Asset identification methodology. Removal of this language, removes the foundation for our Critical Cyber Asset identification methodology. The proposed standard for identifying Critical Cyber Assets is less prescriptive than the existing standard. It is moving in the wrong direction.
Response: Thank you for your comment. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. Similar language to that referred to can be found in the guidance document. Example language is ambiguous and therefore was removed from the standard.				
Chuck B Manning	Electric Reliability Council of Texas, Inc.	2	Negative	ERCOT ISO has joined in the submission of the IRC SRC comments. Please see IRC SRC submission for details.

Balloter	Company	Seg-ment	Vote	Comment
Response: Thank you for your comment.				
Charles H Yeung	Southwest Power Pool	2	Negative	We believe the bright line criteria proposed goes beyond what is required for protecting the bulk power system from cyber attack. We reiterate our support for the ISO RTO Council SRC comments submitted in the comment period.
Response: Thank you for your comment.				
Kim Warren	Independent Electricity System Operator	2	Negative	We appreciate the Drafting Team's reinstatement of Section 4.2.1 pertaining to the exemption of facilities regulated by the CNSC. We however respectfully reiterate our objection to criteria 1.6 and 1.7. In our view, removal of some of the facilities identified as Critical Assets using these criteria will have no impact on the BES. Their inclusion on the Critical Assets list would therefore be unnecessary The Drafting Team's response to our comment was "The inclusion of a risk-based evaluation by any entity would not meet the objective of uniform application of Critical Asset identification across all entities." We must however point out that Criteria 1.3, 1.8 and 1.9 already allow entities (whether they be the RC, the PC etc.) the discretion to designate/identify as Critical Assets, facilities "necessary to avoid BES Adverse Reliability Impacts" or "critical to the derivation of IROLs". Presumably, these entities doing the "designating" will have a documented methodology and apply it. We therefore advocate a similar approach in the case of Criteria 1.6 and 1.7. We believe the list of relevant transmission facilities developed by the Responsible Entity, should be subject to an impact-based assessment by the Reliability Coordinator who has the wide-area view of the system. If necessary, an additional requirement that requires the RC to have a risk-based assessment methodology and to conduct the assessment should be included. Such an arrangement would be akin to the exemption provisions advocated by FERC in its Final Rule on Revisions to the ERO definition of Bulk Electric System. We therefore propose the following specific wording: 1.6 Transmission facilities operated at 500 kV or higher, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.

Balloter	Company	Seg-ment	Vote	Comment
				1.7 Transmission facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations, unless the annual review performed by the Reliability Coordinator (new requirement) demonstrates that destruction, degradation or unavailability of those assets will have no impact outside the local area and will not cause BES instability, separation, or cascading outages.
Response: Thank you for your comment. The SDT considered placing various analysis requirements on the Reliability Coordinator. The Functional Model describes the Reliability Coordinator as "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." However, the nature of the Critical Asset list is long-term, since implementation of CIP-003 to CIP-009 is up to two years. Based on this, it was determined that the Reliability Coordinator was not an appropriate entity for this analysis.				
Kathleen Goodman	ISO New England, Inc.	2	Negative	With regard to Criteria 1.3, ISO-NE agrees with and appreciates the Standard Drafting Team's (SDT) clarification that: "the burden for identifying Critical Assets is with the Responsibility Entity that is the Asset Owner. There is no burden or obligation placed on the Planning Coordinator or Transmission Planner to designate any unit as needed for reliability." (emphases added). To the extent that the Standard Drafting Team continues to leave this type of language in as Criteria 1.3, ISO-NE believes that such explanation should accompany any explanation of the Standard to NERC management/Board and/or FERC to ensure that there is no confusion on this point. ISO-NE continues to believe, however, that Criterion 1.3 should be removed. Because Attachment 1 establishes "bright-line" criteria for what assets should be included as "critical" assets under the Standard, for the reasons previously submitted to the Standard Drafting Team, including a Criterion in the Standard that places the task of making a "criticality" determination on an entity that does not own the assets violates FERC's Order 706 (and its Orders on Rehearing). As previously explained in submitted comments on this Standard, oversight from third parties (such as NERC, or its designee, if NERC so chooses) can be handled through the Rules of Procedure, where liability protections can be properly defined. In this case, of course,

Balloter	Company	Seg-ment	Vote	Comment
				NERC's designee would be entitled to the same liability protections as NERC. With this new iteration of Criteria 1.3, ISO-NE requests its removal, because: (a) it establishes a subjective method not included in other TPL Standards for Planning Coordinator/Transmission Planner (PC/TP) making a determination about generation assets; (b) as FERC has previously stated, PC/TP have no special expertise in identifying which assets are needed to protect as Critical Infrastructure from a cyber-security perspective; and (c) the inclusion of this Criteria may disincentivize generation owners/operators from conducting their own independent analysis – in that they will implicitly rely on whether the PC/TP has informed them of such a designation. Alternatively, such asset owners may simply unilaterally request that their PC/TP make such a designation. In short, the SDT and FERC have recognized the sole responsibility for identifying critical assets rests with the asset owner. As FERC clearly laid out in Order 706 (and its Orders on rehearing), NERC should provide some type of oversight to check that analysis (or designate another type of entity if it is not capable of doing so). Because Criteria 1.3 does not establish "bright-line" criteria for inclusion of bulk power system assets, it should be removed.
Response: Thank you for your comment. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	We thank the drafting team for their efforts and the progress they have made in improving this standard since the last ballot. However, we still believe there are significant issues with the standard. The standard shifts responsibility for critical asset identification to third parties. For example, criterion 1.3 essentially causes generation owners to rely on Planning Coordinators to identify their critical generators. This responsibility should not be trasnferred and Order 706 was clear that it cannot be in paragraph 328. Criterion 1.3 is ambiguous and likely will not result in any generators being identified unless the Planning Coordinator is violating the TPL standards. Adverse Reliability Impact involves impacts to the system that cause separation, cascading, instability, etc. The TPL standards require the Planning Coordinator to plan to prevent these kinds of events for multiple contingencies. Thus, this criterion should be removed.
Response: Thank you for your comment. Criterion 1.3 - The burden for identifying Critical Assets is with the Responsible Entity that is the asset owner. If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D				

Balloter	Company	Seg-ment	Vote	Comment
contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.				
Bruce Krawczyk	ComEd	3	Affirmative	1. When reviewing the changes to the proposed CIP-002-4 standard, do you believe that the proposed standard was responsive to feedback received and provides acceptable bright-line criteria for the determination of Critical Cyber Assets? No Comments: Exelon concurs that the changes made to the CIP-002-4 draft are responsive to the feedback received; however, the current draft version of CIP-002-4 does not address a technical issue previously not identified, and Exelon proposes a modification to the CIP-002-4 language. The current proposed exemption criteria in the "Applicability" Section 4.2.3 states that, "Cyber Assets associated with Cyber Security Plans submitted to and verified by the U.S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54." The wording of the exemption, and the parenthetical information in critical asset criteria 1.1 in Att. 1 (i.e., "including nuclear generation") appear to leave in place the requirement for nuclear generators to comply with Requirement 1, the annual determination of critical assets. Exelon understands that this exemption wording was put in place prior to the NRC letters to both FERC and NERC dated November 26, 2010, that by a matter of policy reserved to NRC the cyber security oversight of the BOP structures, systems, and components (SSCs) with impact on radiological health and safety. Because of the close coupling between electrical power and nuclear power, this regulatory oversight by the NRC would result in no BOP SSCs within the NERC CIP Standards. Thus, restricting the wording of the exemption to cyber assets is unnecessary. Exelon suggests that this technical issue can be resolved by revising the wording of exemption 4.2.3 to mirror that of 4.2.1 for Canadian nuclear generators (i.e., revise to state “4.2.3 Facilities regulated by the U.S. Nuclear Regulatory Commission”). The parenthetical “including nuclear generation” may also be removed from critical asset criteria 1.1 in Att. 1 of the draft standard. It is Exelon’s understanding that the current May 2010 version of the NERC Standard Process Manual, pp. 17-18, allows the draft CIP-002-4 wording to be changed to correct such technical issues without need for re-balloting.
Response: Thank you for your comments. The phrase “including nuclear generation” in Criterion 1.1 is there to define a plant site. Unit output from all units at a single plant site should be included to determine if a plant meets the 1500MW threshold. The evaluation for Critical Cyber Assets is similar. Although it is highly unlikely that nuclear and				

Balloter	Company	Seg-ment	Vote	Comment
non-nuclear units share common Cyber Assets, the evaluation should still occur. The Applicability language serves to ensure that all reliability systems not covered by the NRC will be covered by the CIP standards. The Applicability section has been revised to clarify the nuclear plan exemption.				
David A. Lapinski	Consumers Energy	3	Negative	The revised wording in CIP-002-4, Attachment 1 has not changed adequately to address the ambiguity that we had objected to in our previous comments and negative vote. It would seem that the changes have not done enough to limit inclusion of many more generating units that are part of alternate cranking paths. As this creates ambiguity, the Standard is not acceptable as proposed. In addition, Item 1.5 has not changed in a definitive fashion such as to limit inclusion of only the 'Primary Path", which was the same concern we raised previously.
David Frank Ronk	Consumers Energy	4		
James B Lewis	Consumers Energy	5		
Response: Thank you for your comments. The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2.				
Henry Ernst-Jr	Duke Energy Carolina	3	Affirmative	Yes, however we see much room for improvement and offer the following comments: • Criterion 1.2 – We previously commented that 1000 MVAR was too large, and reiterate that comment again. There are not any reactive resources that large in SERC. Is the drafting team aware of where any 1000 MVAR resources are located? • Criterion 1.3 – This criterion is less clear than before. Adding the phrase "necessary to avoid BES Adverse Reliability Impacts" potentially broadened this criterion to include every last generator on the system, because the defined term "Adverse Reliability Impact" includes tripping of generation. You need to limit this criterion to generation whose loss "could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." • Criterion 1.4 - Need to clarify that this criterion only includes the primary Blackstart Resources. Entities may include various alternative resources in their restoration plans which aren't Critical Assets, but which may not be clearly distinguished from the primary Blackstart Resources in the restoration plan. Add the phrase "that the entity intends to rely on for system restoration".

Balloter	Company	Seg-ment	Vote	Comment
				• Criterion 1.7 – Wording change creates confusion as to whether generating stations are included. Insert the word "transmission" before the word "stations". • Criterion 1.8 – This criterion is less clear than before. Delete the RC, because the identification of facilities to be protected occurs in the planning timeframe. Also the unclear language "critical to the derivation of" and "their associated contingencies" should be struck. Suggested rewording: "Transmission Facilities at a single transmission station or substation location, that are identified by the Planning Authority or Transmission Planner, whose loss could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." • Criterion 1.9 - This criterion is less clear than before. Delete the RC, because the identification of facilities to be protected occurs in the planning timeframe. Also the unclear language "critical to the derivation of" and "their associated contingencies" should be struck. Suggested rewording: "Flexible AC Transmission Systems (FACTS) at a single transmission station or substation location, that are identified by the Planning Authority or Transmission Planner, whose loss could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages." • Criterion 1.10 – Removing the word "directly" creates significant uncertainty regarding what scope of facilities would be included. Reinsert the word "directly", preferably after the phrase "Transmission Facilities". Also, including the word "destroyed" in the phrase "destroyed, degraded, misused or otherwise rendered unavailable" creates significant uncertainty regarding what is intended. Add the phrase "via cyber attack" after the word "unavailable". This will clarify that the evaluation only encompasses destruction, degradation or misuse that can be achieved via cyber attack, and not a physical attack on the facilities. • Criterion 1.12 – The added language is unclear. Suggested rewording: "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements whose loss could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages for failure to operate as designed."

Balloter	Company	Seg-ment	Vote	Comment
				• Criterion 1.13 – As clarified on the Webinar, the language needs to be revised to clarify that the phrase "Each system or Facility" only includes discrete systems or facilities that can individually shed 300 MW or more of load. UFLS and UVLS systems are typically composed of discrete components at many locations (not interconnected), usually on the distribution system. These discrete, localized facilities would not typically interrupt 300 MW individually. • While the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities provides milestones for implementing the CIP standards, we believe that a modification is needed related to the CIP 002 milestones within this plan. The implementation plan presumes that compilation of all of CIP 002 evidence (R1. Application of Methodology; R2. Identification of the new Critical Asset; R3. Identification of the new Critical Cyber Assets; and R4. Annual Approval of the above items) occurs simultaneously for Category 1 and Category 2. This approach does not allow sufficient time for the identification of new Critical Cyber Assets (R3) and approval of the documented CCA list (R4) once new Critical Assets are identified. We believe the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities should be amended to provide a period of 6 months following identification of a new Critical Asset for the identification of new Critical Cyber Assts associated with the new Critical Asset (R3) and the Annual Approval of the revised Critical Cyber Asset List (R4).
Response: Thank you for your comments. Criterion 1.2 - The value of 1000 MVAR used in this criterion is a value deemed reasonable for the purpose of determining criticality. The survey that NERC conducted earlier this year showed that there were facilities that would qualify at this threshold. Criterion 1.3 – Adverse Reliability Impact is defined as "The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection." The Guidance document has been modified to provide additional clarification on this issue. Criterion 1.4 - The SDT considered using the word "primary", but ultimately rejected it as it is not a defined NERC Glossary term in this instance, nor is it used in EOP-005-2. The phrase "that the entity intends to rely on for system restoration" was discussed by the SDT, but it was determined that it added no additional clarity. Criterion 1.7 - The choice of the phrases "Transmission Facilities" and "transmission stations or substations" was intentional to exclude connections and generation only substations. Criterion 1.8 - According to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent				

Balloter	Company	Seg-ment	Vote	Comment
with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion. The wording for criterion 1.8 came from FAC-014-2 Requirement R5. Criterion 1.9 - According to FAC-014-2 Requirement R1 "The Reliability Coordinator shall ensure that SOLs, including Interconnection Reliability Operating Limits (IROLs), for its Reliability Coordinator Area are established and that the SOLs (including Interconnection Reliability Operating Limits) are consistent with its SOL Methodology." Since they have a responsibility to ensure that the IROLs are established and consistent with their SOL methodology, it is valid to list them in this Criterion. The wording for criterion 1.8 came from FAC-014-2 Requirement R5. Criterion 1.10 - Several commenters in the first posting were concerned about the use of the term "directly." After consideration by the Standard Drafting Team, it was determined that the term could be removed without affecting the intent of the criterion. The SDT discussed your suggested changes, and determined the existing language is adequate. The term "destroyed" is listed in the definition of Critical Asset. Criterion 1.12 - The SDT appreciates the suggestion, but believes the posted wording is adequate. Criterion 1.13 - The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. Implementation Plan – Thank you for raising this concern. The SDT will review this implementation plan in the next version and revise as necessary.				
Robert D Adam	Kansas City Board of Public Utilities	3	Affirmative	Consider the changes being proposed in the following language. 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big

Balloter	Company	Seg-ment	Vote	Comment
				iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comments. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system.				
Bruce Merrill	Lincoln Electric System	3	Negative	LES believes the SDT was responsive to much of the feedback received from the industry; however, we question whether these bright-line criteria as a whole are acceptable for determining Critical Cyber Assets. We believe a few criteria need to be adjusted to provide a proper foundation moving forward, and support the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS) to properly address these issues.
Dennis Florom	Lincoln Electric System	5		
Eric Ruskamp	Lincoln Electric System	6		
Response: Thank you for your comments.				

Balloter	Company	Seg-ment	Vote	Comment
Charles A. Freibert	Louisville Gas and Electric Co.	3	Affirmative	PPL affiliates appreciate the hard work and efforts of the Standards Drafting Team in reaching this point in the standards development process. However PPL affiliates have reviewed the CIP-002-4 standard version dated 11/30/2010 and the associated Rationale and Implementation Reference Document and Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and still find the need to offer comments as follows: 1) CIP-002-4, Attachment 1, Criterion 1.1 should include a requirement that the Generator Owner or Generator Operator must inform the Transmission Operator, Transmission Operator, Planning Coordinator or Transmission Planner of each group of generating units that has been designated as a critical asset. 2) CIP-002-4, Attachment 1, Criterion 1.3 should be reworded to indicate "Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator, "and the Transmission Owner and Transmission Operator" as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon. 3) CIP-002-4, Attachment 1, Criterion 1.5 should be reworded to indicate "The facilities comprising the Cranking Paths and Meeting the initial switching requirements from the Blackstart Resource “up to and including” the first interconnection point of the generation unit(s) to be started, or up to “and including” the point on the Cranking Path where two or more path options exist "including the first interconnection point of the generation unit(s) to be started" , as identified in the Transmission Operator's restoration plan. 4) CIP-002-4, Attachment 1, Criterion 1.13 should be revised to include load shed systems capable of shedding 300 MW or more. These load shed systems, which are typically part of the energy management systems, are initiated to ensure the reliability of the BES. 5) CIP-002-4, Attachment 1, Criterion 1.13 should be reworded to indicate that distributed UFLS or UVLS schemes (i.e., individual UF or UV relays operating independently in multiple substations) are not considered to be a critical asset. Collectively the UFLS or UVLS scheme may shed more than 300MW; however, due to the distributed nature of the scheme, the UFLS or UVLS schemes are not considered to be a critical asset.
Response: Thank you for your comments. Criterion 1.1 - It is agreed that communication between Generator Operators and Transmission Owners and Transmission Operators will be required to ensure that all Critical Assets are identified.				

Balloter	Company	Seg-ment	Vote	Comment
Criterion 1.3 - The process would be that the Planning Coordinator or Transmission Planner would notify the Generation Owner and Generation Operator about any facilities that meet Criterion 1.3. The GO and/or GOP would need to notify the Transmission Owner of any facilities that need to be considered for Criterion 1.10. Criterion 1.5 - The SDT appreciates the suggestion, but believes the posted wording is adequate. Criterion 1.13 – A discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. During the previous ballot and comment period, the SDT received many comments on this criterion, whose wording was similar to this suggestion. Some commenters stated that the wording of this criterion will inadvertently bring in all SCADA systems with the capability of shedding load even if such SCADA systems are in fact not planned or operated to perform load shedding. This was not the intent of the SDT. Other commenters stated that this item needs to be clarified to confirm that it applies to a single common control system only, and not multiple but separate "like" systems that in aggregate are capable of load shedding up to 300 MW. Also, the criterion needs to be clarified to confirm that it applies to systems "configured" for automatic load shedding, not simply just "capable" of load shedding. This criterion was intended to include as Critical Assets regional Under Frequency Load Shedding and Under Voltage Load Shedding schemes. The SDT appreciates the suggestion, but believes the posted wording is correct.				
Darl Shimko	Madison Gas and Electric Co.	3	Abstain	We appreciate the Standard Drafting Teams time and effort in developing this revised Standard and believe substantial progress has been made. However, there are several items that we feel warrant further modifications. 1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan. Minor modifications are required for 1.4. As currently drafted, any Blackstart Resource identified in the Transmission Operator's restoration plan would be a Critical Asset without regard to the circumstances of the Blackstart Resource. A modified approach would be to allow the Transmission Operator to have both essential and non-essential resources (resources that meet the CIP bright-line criteria and those that do not meet the CIP bright-line criteria) within their restoration plan. We recommend that Criterion 1.4 be rewritten to state: Each Blackstart Resource identified as being necessary to restore the system in the Transmission Operator's restoration plan. Rationale: By modifying the criterion, the Transmission Owner is able to develop a fully encompassing plan that will allow resources with blackstart capability to be included in the plan, even if that particular resource is not deemed to be essential to the restoration of the system. This would add diversity to the restoration plans, allowing the
Joseph G. DePoorter	Madison Gas and Electric Co.	4		

Balloter	Company	Seg-ment	Vote	Comment
Steven Schultz	Madison Gas and Electric Co.	5		Transmission Operator to use all the available resources to ensure the reliability of the system during these circumstances. When a Blackstart Resource is included in the plan, it will receive the full attention of the Transmission Operator and will be the focus of training and emergency simulation. Without this modification, it is likely that Blackstart Resources that are not essential, but may be helpful to the restoration plan, will not be included in the plan and therefore will not be a considered during the training and simulation drills. The Transmission Operator will likely be in a better position to respond to the circumstances, which may be unforeseen, if it has included all available resources, not just those deemed critical. 1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program. Clarity is required for 1.13. The owner of a UFLS system is not listed in the applicability section of this Standard which is a Distribution Provider. PRC-008-0 has the Distribution Provider in its applicability section for the maintenance and testing of UFLS relays. Please review and update. This criterion could be interpreted as each relay that is enabled to perform UFLS operations would be considered a CA. These relays are located at distribution substations and may change annually due to the customer make up per distribution feeder. Since a UFLS system is enabled at individual feeder relays, this criterion would require each individual relay to be classified as a CA. When the NERC defined term of "Facility" is in the criterion it will bring in all components of the UFLS system as being a CA. We recommend that Criterion 1.13 be rewritten to state: Each automatic load shedding relay that interrupts, without human operator initiation, 100 MW or more of load as a result of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program. Rationale: The 300 MW limit is a DOE requirement and is subject to public law outside the authority of NERC. The 100 MW is per FERC approved NERC Standard EOP-004-1. UFLS relays that fall below this threshold will still need to be maintained per PRC-008-0 since there is no bright line associated with that Standard. This recommended revised criterion adds to the adequate level of reliability and does not adversely affect those small entities. 1.15 Each control center or backup control center used to control generation at multiple plant
Jeffrey M Keebler	Madison Gas and Electric Co.	6		

Balloter	Company	Seg-ment	Vote	Comment
				locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection Even if a small utility, as a joint owner, has control over only a small portion of a large plant that falls under the brightline of 1.1, we are concerned that as currently written, the first sentence of this criteria would unintentionally designate this small utility's control center as critical. We would propose rewording the criteria as follows: Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.3 or 1.4, or used to control at least 1500 MW of generation at any Facility identified in criteria 1.1. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. Rationale: The important part of this criteria is the amount of generation controllable by the system, the MW level of the entire generation. As written, it could be interpreted that the total generation size at a single plant location is the defining criteria, not what is controllable by the individual system. If a system is only able to control 100 MW of a 2000 MW plant, the Criteria for 1.15 should be looking at the 100 MWs of control capability, not the 2000 MW plant.
Response: Thank you for your comments. Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. Criterion 1.13 – The SDT does not feel it necessary at this time to include Distribution Providers in the Applicability section but may consider this in future revisions of the Standards. Distribution Providers may own certain very limited BES Cyber Assets, generally limited to UFLS and UVLS relays. However, additional functional entities (i.e. Transmission Operators) generally provide aggregate control of these relays. Criterion 1.15 - The concern here is that the smaller utility's control center could provide a path to compromise the functionality of the generation designated a Critical Asset.				
Rick Keetch	NRG Energy Power Marketing, Inc.	3	Negative	The revision to CIP002 V4 Section 1.15 in Attachment 1 still requires additional clarification. The requirement states that if a facility has the ability to control generation at multiple locations, it is designated as a control center and therefore is deemed critical under this requirement. However, a single entity that has generation may have a control room that controls remote sites from a single location (ex. Gas turbines). If the intent is to pull in these assets under the classification of control center, it should clearly state that control rooms having this configuration are in scope or redefine the control center definition based upon application of this methodology.
Richard Comeaux	LaGen	4		

Balloter	Company	Seg-ment	Vote	Comment
Patricia A. Lynch	NRG Energy, Inc.	5		
Response: Thank you for your comments. Criterion 1.15 - From the posted Guidance document: "A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction." If the control center meets the specifications of criterion 1.15, it is a Critical Asset.				
Scott Peterson	San Diego Gas & Electric	3	Negative	SDG&E is concerned that the "bright line" needs additional improvement to make sure it is clear to all entities. Comment on 1.8, 1.9, 1.10: There should be some obligation that the parties that identify the Transmission Facility (e.g. RC, PA, TP, GO) as critical also notify the Transmission Owner and Operator of that identification so the TOP and TO are aware and can protect. Comment on 1.8, 1.9: What does the statement "critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies" mean? This isn't clear.
Response: Thank you for your comments. Criterion 1.8 and 1.9 - FAC-014-2 R5 contains all of the information concerning communication of Facilities that are critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. Criterion 1.10 – It is agreed that communication between Generator Operators and Transmission Owners and Transmission Operators will be required to ensure that all critical Assets are identified. The wording for 1.8 and 1.9 came from FAC-014-2 Requirement R5.				
James R. Keller	Wisconsin Electric Power Marketing	3	Affirmative	We appreciate the diligence of the Standard Drafting Team in reviewing and responding to the comments and feedback provided during the previous ballot, and the changes made to the bright line criteria in Attachment 1 in response to comments and feedback. We strongly support the change to a single implementation timeline of 24 months which will simplify both implementation and audit requirements, and would like to point out the fact that there is a discrepancy in timelines specified in the draft standard and the timelines specified in the draft implementation plan. This discrepancy must be corrected in the final implementation.
Linda Horn	Wisconsin Electric Power Co.	5		

Balloter	Company	Seg-ment	Vote	Comment
Anthony Jankowski	Wisconsin Energy Corp.	4		Also, the timeline proposed for CIP-005-4 should coincide with the timeline for the other CIP version 4 standards to further streamline compliance and audit processes. We would also like to express concern that, in so much as Criterion 1.1 could result in the identification of generation plant locations with no Critical Cyber Assets, the resulting requirements in Criterion 1.10 could result in expending efforts protecting transmission assets that might not otherwise need to be protected, diverting resources that might be more effectively expended elsewhere. Finally, we would like to express concern that the failure to specify a criticality criteria for Blackstart Resources in Criterion 1.4 will result in current blackstart-capable units not being identified as Blackstart Resources. Thank you for your consideration of these comments.
Response: Thank you for your comments. The flowchart in the implementation plan has been removed. Your comments on CIP-005-4 will be forwarded to that team. Criterion 1.10 - The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets. Any Transmission Facility that the loss of which would result in the loss of a Critical Asset identified in criterion 1.1 or 1.3 would need to be classified as a Critical Asset. Criterion 1.4 - The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				
Kenneth Goldsmith	Alliant Energy Corp. Services, Inc.	4	Negative	Alliant Energy agrees with most of the revisions, except criterion 1.4 concerning Blackstart units. We are very concerned that with the wording as in the standard, many Registered Entities will not make their emergency generation available as blackstart resources, and the end result will be a reduction in the reliability of the BES. A possible solution is to consider a Blackstart Tier Methodology, where "Primary" Blackstart units would be subject to the full CIP criteria, and then "secondary" Blackstart units that would not be required to meet the full requirements due to their size and negligible impact on the BES.
Response: Thank you for your comments. A tiered approach to Blackstart Resources is a good idea, and the drafting team suggests that a SAR be submitted by the entity outlining this approach to EOP-005-2. It is beyond the scope of this SDT.				

Balloter	Company	Seg-ment	Vote	Comment
Timothy Beyrle	City of New Smyrna Beach Utilities Commission	4	Affirmative	Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, not matter the importance to the region. This is not reasonable and only a few for the region ought to be identified (e.g., as identified in the regional plan). Unfortunately, not all regions have restoration plans, which is really the issue (which seems a violation to EOP-006-1 R3 to me).
Response: Thank you for your comments. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				
Thomas W. Richards	Fort Pierce Utilities Authority	4	Affirmative	Although we are voting affirmative, FPUA strongly agrees with APPA's comments, which state: In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following rewording: 1.4. Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than an aggregate of 1500 MW in a single Interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's				

Balloter	Company	Seg-ment	Vote	Comment
restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Jack Alvey	Indiana Municipal Power Agency	4	Affirmative	IMPA is voting affermative on the ballot, however, there is an issue that needs to be addressed and corrected. In Attachment 1, criteria 1.4 (Blackstart Resources), it is including all Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. Basically, criteria 1.4 eliminates all exceptions under criteria 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. To address this issue, IMPA proposes to make the following edits to 1.4 and 1.5: 1.4 Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than aggregate of 1500MW in a single interconnection. 1.5 The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4 to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation - and thento wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. IMPA also recomments using different wording than just annual. We would prefer to see wording

Balloter	Company	Seg-ment	Vote	Comment
				that might say "each calendar year but no longer than 16 months" to avoid the ambiguityh of the term "annual."

Response: Thank you for your comment.
The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." These comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.

Balloter	Company	Seg-ment	Vote	Comment
Christopher Plante	Integrys Energy Group, Inc.	4	Affirmative	Wisconsin Public Service Corporation and Upper Peninsula Power Company support the MRO's NSRS comments. However, we are concerned with Attachment 1, Criterion 1.13. As currently worded, this criterion could unintentionally designate multiple smaller, disparate systems with like settings as a "system" that performs automatic load shedding of 300 MW or more, assuming the total combined load shedding capability of the disparate systems exceeds 300 MW. To prevent this, we would propose rewording the criterion as follows to more closely match the old version: Each COMMON system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.
Response: Thank you for your comments. A discrete component that sheds more than 300MW of load due to the implementation of Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program is a Critical Asset. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. It is unclear how adding the term "common" adds any additional clarity over the existing wording.				
Jeff Mead	City of Grand Island	5	Negative	Comments put in official form.
Response: Thank you for your comments.				
Amir Y Hammad	Constellation Power Source Generation, Inc.	5	Affirmative	Constellation appreciates the hard work and dedication of the CSO 706 Standard Drafting Team. Constellation Power Generation believes that the Standard Drafting Team needs to further explain the technical justification for the 1500 MW bright-line threshold in Attachment 1 – 1.1 as well as the 300 MW bright-line threshold in Attachment 1 – 1.13. The technical justifications should be included in the guidance documentation. Constellation Energy Nuclear Group appreciates the inclusion of the language in 4.2.3: "Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54." This exemption language should

Balloter	Company	Seg-ment	Vote	Comment
				also be added to CIP-003 thru -009.
Response: Thank you for your comments. The SDT believes that the justification for each threshold is presented in the guidance document. The posted Guidance document has been modified to add reasoning for the 300MW threshold level. The exemption language referenced is in the posted versions of CIP-003-4 to CIP-009-4.				
Kenneth Dresner	FirstEnergy Solutions	5	Affirmative	No Comments
Response:				
Brent Hebert	Horizon Wind Energy	5	Negative	The way 1.15 is written, it would include control centers that control 1500 MW of total generation in an Interconnection comprised of small generators dispersed throughout multiple Balancing Authorities and Reserve Sharing Groups within that Interconnection. We believe this criteria is too broad, does not meet the intent of enhancing reliability, and places a significant burden on small entities that control dispersed generation. We believe using a criteria based on the amount of generation controlled within a single BA or RSG would better enhance reliability, while not unduly burdening entities that cannot appreciably contribute to resolving BES emergencies. We recommend changing the criteria from "Each control center or backup control center used to control generation equal to or exceeding 1500 MWs in a single Interconnection." to "Each control center or backup control center used to control total generation in a single BA or RSG equal to or exceeding the lesser of: •1500 MWs, or •The Most Severe Single Contingency for that BA RSG.
Response: Thank you for your comment. The SDT appreciates the suggestion, but believes the posted wording is adequate.				

Balloter	Company	Seg-ment	Vote	Comment
Mike Laney	Luminant Generation Company LLC	5	Affirmative	Luminant thanks the STD for their work on the standard and for the opportunity to provide comments for consideration by the SDT. Luminant believes the changes to CIP-002-4 are responsive to the concerns expressed by the industry and provide acceptable bright-line criteria for the determination of Critical Assets. Luminant does request the SDT to consider a wording change in the "Draft Guidance Document". On page 10 of the Clean version of the document, in reference to Special Protection Schemes, the following is listed: "Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time they are required or if they operate outside of the parameters they were designed for. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets. " (emphasis added) The term "implemented" is not consistent with other NERC standards and can lead to disagreements on who is responsible for the Critical Asset CIP requirements. Luminant asks the SDT to change the language to: "Generator Owners and Operators that own such systems and schemes…." The term "own" is consistent with other NERC standards that are applicable to Special Protection Systems and Remedial Action Schemes, and very clearly identifies the responsible entity. Thank you for your consideration of our comments.
Brad Jones	Luminant Energy	6		
Response: Thank you for your comments. Your suggested change to the Guidance document has been made.				
Don Schmit	Nebraska Public Power District	5	Affirmative	Suggest changing Attachment 1, sub-paragraphs 1.4 and 1.5 to read as follows: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path

Balloter	Company	Seg-ment	Vote	Comment
				options exist, as identified in the Transmission Operator's restoration plan.
Response: Thank you for your comments. Criterion 1.4 – The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. The SDT appreciates the suggested wording, but believes the posted wording is adequate.				
Michelle DAntuono	Occidental Chemical	5	Affirmative	Request clarification where Attachment 1, 1.3 allows PCs or TPs to designate units that are necessary to avoid "BES Adverse Reliability Impacts". Is this meant to be RMR units?
Response: Thank you for your comments. The units are not necessarily designated as reliability must run. If the PC or TP has identified Adverse Reliability Impacts (the impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection), then any units identified that avoid this scenario must be classified as a Critical Asset.				
Joanna Luong-Tran	TransAlta Centralia Generation, LLC	5	Abstain	For the criterion 1.1, the SDT response said "the guidance document posted by the SDT provides directions on the location issue". We have reviewed the guidance document and we think the terms of "a defined physical footprint" and "commonly accepted generating facility terminology" in the SDT response are still vague. Can the SDT elaborate this by providing some examples? For the criteria 1.6 and 1.7, we have read the SDT response and think the Generator Interconnection Facilities as defined in the NERC project http://www.nerc.com/filez/standards/Project2010-07_GOTO_Project.html, should be excluded from the Transmission Facilities, the term used in the criteria 1.6 and 1.7. The guidance document discusses this. We think it is appropriate to clarify this in the standard, instead of addressing this in the guidance document.
Response: Thank you for your comments. Additional clarity has been added to the Guidance document. The following sentence was added to the language explaining criterion 1.1: “Single plant location refers to a group of generating units occupying a defined physical footprint, often but not always, these units are surrounded by a common				

Balloter	Company	Seg-ment	Vote	Comment
fence, have a common entry point, share common facilities such as warehouses, water plants and cooling sources, follow a similar naming convention (plant name - unit number) and fall under a common management organization." The SDT believes that the Guidance document is the appropriate place for this discussion until the Generation Interconnection Facilities are incorporated into the standards.				
Brenda Powell	Constellation Energy Commodities Group	6	Negative	Constellation appreciates the hard work and dedication of the CSO 706 Standard Drafting Team. Constellation Energy Commodities Group continues to be concerned that Attachment 1, criteria 1.15 inappropriately covers control centers in one-size fits all approach. While there are EMS systems that can directly control generation, there are also Generation Management Systems (GMS) that function on a much lower level. For instance, many GMS systems: • Do not open and close breakers of any critical asset • Simply send a signal to units operating in the AGC mode and do not directly move the units output • Can only request MW movement between those ranges. Each generating unit controls the set points (low and high AGC limits and ramp rates). • May be turned off and/or switched locally to manual dispatch mode without disruption to the BES. If, through malicious means, attempts are made to use the GMS to adversely impact the reliable operation of a generating unit, the generating unit would be taken off of AGC. No single aspect of system operations should be viewed in a vacuum. By design, multiple points of system information are processed and reacted to in context of each other. Mechanical and human checks and balances react to data to maintain a responsive, reliable system. Should the data become compromised for some reason operators will react to the disparities by switching to manual or other operational measures. Requirement 2 distinguishes critical cyber assets as "shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. The control centers covered under criterion 1.15 should also include the same distinction. In addition, defining the control center area would be more appropriately determined by

Balloter	Company	Seg-ment	Vote	Comment
				planning studies, none of which are as broad as a single Interconnection. Since this may create complications for standard applicability, we propose that the area be set by NERC Regional area. 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. For the above reasons, we propose the following revision: 1.15 Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW of generation in a single NERC Regional area.
Response: Thank you for your comments. The SDT considered your proposed wording. In order for the plant to determine that if, "through malicious means, attempts are made to use the GMS to adversely impact the reliable operation of a generating unit, the generating unit could be taken off of AGC," it is felt that the protections provided in CIP-003 to CIP-009 are necessary. In addition, the SDT believes that the generation summary must be performed at the NERC Interconnection, because control actions are not taken at the NERC Regional level.				
Larry W. Rodriguez	Entegra Power Services	6	Negative	FERC & NERC must attempt to provide the security needed, BUT in a way that balances adequate security with an entities ability to absorb the enormous costs! We are a small shop IPP which can not pass on these costs to ratepayers as the IOUs. The up front "Brightline" costs and ongoing costs MAY PUT US OUT OF BUSINESS and reduce jobs in a terrible economic time for the entire country. Please consider some efforts to balance adequate security needs with the size and financial capability of companies.
Response: Thank you for your comments.				

Balloter	Company	Seg-ment	Vote	Comment
The SDT and volunteer industry participants have developed appropriate Critical Asset Identification criteria which have been presented to industry through various iterations for review and feedback. In addition, the SDT has attempted to factor in this issue by limiting the scope of Critical Cyber Assets to those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.				
Joseph O'Brien	Northern Indiana Public Service Co.	6	Affirmative	Concerns included in previous ballot have been addressed
Response: Thank you for your comments.				
Jim R Stanton	SPS Consulting Group Inc.	8	Negative	While the changes in the Criteria 1.3 allow generators to be informed of whether they are designated a Critical Asset by the Planning Coordinator or Transmission Planner, that was not the point. The discretion to make such designations without proper due diligence or independent review remains. Planning studies have a wide latitude of assumptions and it would be quite easy designate one's competitor as critical and employ the assumptions in the planning models to make that happen. Lacking independence at the PC and TP level, independent review is the only way to insure competition is not blunted by this ability to designate one's competitor as critical.
Response: Thank you for your comments. In the Functional Model, one of the tasks of the Planning Coordinator is "Facilitates the integration of the respective plans of the Resource Planners and Transmission Planners within the Planning Coordinator area. a. Reviews the integrated plan with respect to established reliability needs considering the impact on and by adjoining systems. b. In coordination with the Resource Planners and Transmission Planners, facilitates the development of alternative solutions for plans that do not meet those reliability needs." One of the alternative solutions developed may require the availability of a particular generator to meet reliability needs and avoid an Adverse Reliability Impact. Likewise, one of the tasks of the Transmission Planning function is "Evaluate, develop, document, and report on expansion plans for the Transmission Planner area. Assess whether the integrated plan meets reliability needs, and, if not, report on potential network conditions or configurations that do not meet performance requirements." If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.				

Balloter	Company	Seg-ment	Vote	Comment
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Affirmative	Many Canadian members of NPCC are of the opinion that in Attachment 1 of the draft CIP-002-4 standard an RC led exclusion provision should be available to allow some facilities to be exempted from the CIP standards. Also the designation of a PC in Attachment 1 in the criteria "1.3" should be removed as there is a liability issue for the PC that fails to correctly identify a GO GOP as being impactive. The TP is the appropriate entity, and correctly identified, to do this and is more likely to have the necessary information in interconnection agreements and design specifications coordinated at the local level.
Response: Thank you for your comments. The SDT believes that having an exception process to the criteria presents the same challenges associated with a risk-based assessment in external review and oversight. One of the functions identified in the Functional Model is Planning Reliability, which has an identified task of "Evaluate, develop, document, and report on resource and transmission expansion plans for the Planning Coordinator area. Integrate the respective plans, evaluate the impact of those plans on and by adjoining Planning Coordinator's integrated plans and assess whether the integrated plan meets reliability needs, and, if not, then to report on potential transmission system and resource adequacy deficiencies and suggest or facilitate the process for developing alternative plans to mitigate identified deficiencies." The Functional Entity responsible for that function is the Planning Coordinator, who is "(t)he functional entity that coordinates, facilitates, integrates and evaluates (generally one year and beyond) transmission facility and service plans, and resource plans within a Planning Coordinator area and coordinates those plans with adjoining Planning Coordinator areas." Another function in the Functional Model is Transmission Planning, which has an identified task of "Evaluate, develop, document, and report on expansion plans for the Transmission Planner area. Assess whether the integrated plan meets reliability needs, and, if not, report on potential network conditions or configurations that do not meet performance requirements and provide potential alternative solutions to meet performance requirements." The Functional Entity responsible for that function is the Transmission Planner, who is "(t)he functional entity that develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within a Transmission Planner area." The Reliability Coordinator, on the other hand, is "The functional entity that maintains the Real-time operating reliability of the Bulk Electric System within a Reliability Coordinator Area." The focus of Criterion 1.3 is the long-term planning horizon, not real-time.				
Stacy Dochoda	Southwest Power Pool Regional Entity	10	Affirmative	1) Criteria 1.5 can be read to limit the cranking path to only the path between the entity's own defined blackstart resource and the generation resource to be started. This fails to consider the situation where cranking power is obtained through a tie interconnection to an adjacent utility or generation owner/operator. In this instance, the cranking path needs to be defined as starting at the interconnect point substation, in effect making the adjacent utility the blackstart

Balloter	Company	Seg-ment	Vote	Comment
				resource. If not clarified, a number of entities could identify no cranking paths to generation that must be started as part of initial system restoration simply because they have no blackstart generation resources that they, themselves, own and/or operate. 2) It is still not clear as to how far blackstart must go before initial system restoration is complete. Black start should be defined as starting the entity's generation resources to the point that load can be served (not to be confused with bringing on load to balance generation during the black start sequencing). This is often more than starting the first "black start" combustion turbine unit to start a thermal unit. Unless that black start unit has sufficient capacity to start individually every other generation resource in the entity's footprint that is not self-starting, additional generation is required even if not specifically identified as a black start resource in the entity's restoration plan. 3) There is sufficient opportunity for confusion and interpretation of the term Control Center that if the term is not to be added to the NERC Glossary, it should be defined locally to the standard. 4) Criteria 1.10 should be modified to refer to Critical Assets. In other words, "…would result in the loss of the Critical Assets..." 5) Criteria 1.14, 1.15. and 1.16 should refer to control center "and" backup control center rather than "or." 6) Measure M1 should be modified to state "The Responsible Entity shall make available its approved list of Critical Assets as specified in Requirement R1." (addition of the word "approved") 7) Measure M2 should be modified to state "The Responsible Entity shall make available its approved list of Critical Cyber Assets as specified in Requirement R2." (addition of the word "approved")

Balloter	Company	Seg-ment	Vote	Comment
				8) The Responsible Entity data retention requirement (Section D.1.4.1) should be modified to require records to be kept since the effective date of the standard or the most recent scheduled audit of this version of the standard, whichever is a shorter period of time, unless a shorter retention period (such as the 90-day routine log retention found in several of the CIP standards) is specified in a requirement. This is in keeping with NERC Compliance Process Bulletin #2009-005 'Current In-Force Document Data Retention Requirements for Registered Entities'. A similar modification should be made to CIP-003-4 through CIP-009-4. (Entities are already expected to retain all evidence in support of the annual, or in the case of the CIP standards to date, semi-annual self certification, so this is not an undue burden. Retention of records with the exception of specific information with a prescribed shorter retention, such as logs, will allow the CEA to verify sustained compliance with the standards over the full audit period. And, in the case of the logs, the entity will need to maintain some sort of evidence that logs were retained for at least 90 days, although retention of the actual logs is not required.) 9) Requirement R1 should be clarified to require the first list of identified Critical Assets to be developed prior to the effective date of the Standard. A number of entities have adopted the position that an annual requirement allows the first instance of the requirement to be performed any time within the first year after the effective date. 10) Requirement R2 should be clarified to require the first list of identified Critical Cyber Assets to be developed prior to the effective date of the Standard. A number of entities have adopted the position that an annual requirement allows the first instance of the requirement to be performed any time within the first year after the effective date. 11) The first bulleted qualifying criterion found in Requirement R2 states “The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter.” Although well intentioned, this does not adequately address risk exposure. While a given Critical Cyber Asset might not communicate itself with Cyber Assets outside of the Electronic Security Perimeter, the network it is connected to may well have connectivity to external networks. That external connectivity offers a vector for compromise through an intermediary system that both the external network and the Critical Cyber Asset are connected to. This exclusion should only apply

Balloter	Company	Seg-ment	Vote	Comment
				in the instance where the network employing a routable protocol is completely isolated from any network not enclosed within the same Electronic Security Perimeter. 12) A number of entities are getting around the routable protocol criteria for Critical Cyber Assets in Requirement R2 by utilizing data diodes for communication. This issue desperately needs to be addressed in this revision of the requirement. 13) Requirement R3 should be modified to require any update of the Critical Asset or Critical Cyber Asset list to be approved. This activity should be separated from the required annual review and approval, where the approval is required even if no changes were identified. 14) The proposed effective date of eight calendar quarters after regulatory approval (or the first day of the ninth calendar quarter after NERC BoT approval where regulatory approval is not required) is excessive and should be reverted back to the original two calendar quarter specification. The expectation is that the first Critical Asset and Critical Cyber Asset list must be developed by the effective date and allowing two years given straightforward bright-line criteria is not reasonable. While the concern may be that the entities would be expected to be fully compliant with all requirements of all eight standards by the effective date, such is not the case. Entities are expected to maintain compliance for any currently identified Critical Cyber Assets that appear on the Critical Cyber Asset list under the bright-line criteria. The entity then has up to two years to bring into compliance any newly identified Critical Cyber Assets stemming from the Version 4-compliant Critical Cyber Asset list. With an eight-calendar quarter effective date, entities can logically assume that they would have up to four years to come into compliance. 15) Figure 1: Sample Implementation Plan Timeline (General Case) in the accompanying guidance document should be restored to clarify the compliance timeline issue discussed in the previous comment.

Response: Thank you for your comments.

1. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." Additionally, it should be noted that

Balloter	Company	Seg-ment	Vote	Comment
				EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." 2. Again, A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." 3. Since the term "control center" is used in other NERC standards without confusion, it can be reasonably expected that a commonly accepted industry definition exists. The SDT believes that defining this term under this proposed version of the Standard would have far-reaching impacts beyond the scope of CIP-002-4 to CIP-009-4. 4. The SDT has considered your proposal and believes the posted wording is adequate. 5. The SDT has considered your proposal and believes the posted wording is adequate. 6. Since the list may be updated between annual approvals, the most updated list should be provided for Measure M1. 7. Since the list may be updated between annual approvals, the most updated list should be provided for Measure M2. 8. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. The suggested changes to the data retention requirement will be considered in a subsequent version of the CIP standards. 9. In order to be compliant with CIP-002-4 on the effective date of the standard, the list must be developed by the effective date. This is clarified in the implementation plan. 10. In order to be compliant with CIP-002-4 on the effective date of the standard, the list must be developed by the effective date. This is clarified in the implementation plan. 11. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. This issue will be considered in a subsequent version of the CIP standards. 12. The scope of CIP-002-4 was to address the consistency issues with the Critical Asset identification method. The team deliberately limited the scope of changes in this interim standard to minimize the impact on the industry while addressing the identified consistency issues. This issue will be considered in a subsequent version of the CIP standards. 13. The SDT debated this issue and determined that an annual approval of each list was sufficient. 14. Currently identified CCAs which would remain on the list after applying "bright-line" criteria should comply with Version 3 of the CIP Cyber Security Standards until the Effective Date of Version 4. CCAs identified through the first application of Attachment 1 of CIP-002-4 shall comply with Version 4 of the CIP Cyber Security Standards on the Effective Date as well. In essence, an entity should have their list of CCAs fully compliant with Version 4 of the CIP Cyber Security Standards on the Effective Date, which occurs approximately 2 years after FERC approval in the US. 15. Currently identified CCAs which would remain on the list after applying "bright-line" criteria should comply with Version 3 of the CIP Cyber Security Standards until the Effective Date of Version 4. CCAs identified through the first application of Attachment 1 of CIP-002-4 shall comply with Version 4 of the CIP Cyber Security Standards on the Effective Date as well. In essence, an entity should have their list of CCAs fully compliant with Version 4 of the CIP Cyber Security Standards on the Effective Date, which occurs approximately 2 years after FERC approval in the US.

Balloter	Company	Seg-ment	Vote	Comment
Larry D. Grimm	Texas Reliability Entity	10	Affirmative	In Part D, Compliance, Section 1.2, the acronyms RE and CEA should be spelled out (Regional Entity and Compliance Enforcement Authority).
Response: Thank you for your comment. Your suggested changes have been made.				
Louise McCarren	Western Electricity Coordinating Council	10	Affirmative	We recognize that the drafting team was charged with developing a bright line methodology for determining Critical Assets to address the need for consistency and that the bright line methodology accomplishes that. We continue to have concerns that for some entities in the West, the bright line methodology may result in fewer facilities being identified as Critical Assets than under the entities individual methodologies required by the current version of CIP-002. We also continue to have concerns that the proposed standard is not as clear as it could be regarding the identification of Critical CYBER Assets and urge NERC to consider a bright line methodology for Critical CYBER Assets in future revisions of the standard.
Response: Thank you for your comments. While some entities may have a few assets fall off of its Critical Asset list, it is expected that overall more BES assets in North America will be classified as Critical Assets. This issue will be considered in a subsequent version of the CIP standards.				
Frank Gaffney	Florida Municipal Power Agency	4	Affirmative	FMPA appreciates the hard work of the SDT. We have five issues that were not a big enough reasons to vote Negative, but, we would like to see addressed: 1. On Attachment 1, bullet 1.12, the phrase "for failure to operate as designed" was added since the last posting. We believe that this is inappropriate. Most SPS's are installed for automatic response to multi-contingency events. For an IROL to be exceeded, the multi-contingency event would need to occur at system conditions that would cause an IROL to be exceeded at the same time that the SPS failed to operate. The probability of the multi-contingency event occurring at such system conditions is very small (e.g., 1 in 50 year order of magnitude frequency), and the SPS would need to fail at that same time. We believe that the appropriate risk to protect against is manipulation of SPS at conditions experienced more frequently and we believe the original wording is correct.. 2. Attachment 1, bullets 1.4 and 1.5. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the region's black-start unit and cranking paths ought to be
David Schumann	Florida Municipal Power Agency	5		
Richard L. Montgomery	Florida Municipal Power Agency	6		

Balloter	Company	Seg-ment	Vote	Comment
				identified as critical (e.g., as identified in the regional plan). FMPA suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3. 3. Use of the word "annual". We would probably be better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term "annual". 4. 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the combined Contingency Reserves of entities within the Reliability Coordinator or something like that 5. Attachment 1, bullet 1.13 Automatic load shedding of 300 MW. The 300 MW is rather arbitrary and it ought to be any cyber-system controlled ability to shed load, not just automatic, of the same target of 1.1 (currently 1500 MW). Loss of 300 MW of load has less impact to BES reliability than loss of 300 MW of generation, so, there is inconsistency between the 1500 MW target for generation of bullet 1.1 and the 300 MW loss of load target of 1.13.
Response: Thank you for your comments. 1. "Failure to operate as designed" was added to this criterion to account for human error, misconfigurations, improper change management (whether unintentional or malicious). 2. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. 3. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. 4. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. 5. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. The posted Guidance document has been modified to add reasoning for the 300 MW threshold level.				
Larry E Watt	Lakeland Electric	1	Negative	We appreciate the hard work of the SDT. We have four issues that we would like to see addressed: 1. Use of the word "annual". We would probably better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term.

Balloter	Company	Seg-ment	Vote	Comment
				2. 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the combined Contingency Reserves of entities within the Reliability Coordinator or something like that 3. Automatic load shedding of 300 MW. The 300 MW is arbitrary and it ought to be any cyber-system controlled load shedding, not just automatic, of the same target of 1.1 (currently 1500 MW) 4. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the regions black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). FMPA suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3.
Response: Thank you for your comments. 1. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. 2. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. 3. The posted Guidance document has been modified to add reasoning for the threshold level. 4. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				
Gregg R Griffin	City of Green Cove Springs	3	Affirmative	Use of the word "annual", probably better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the contingency reserves of the Reliability Coordinator or something like that Automatic load shedding of 300 MW. The 300 MW is arbitrary and it ought to be any load shedding of the same target of 1.1 (currently 1500 MW) Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, not matter the importance to the region. This is not reasonable and only a few for the region ought to be identified (e.g., as identified in the regional plan). Unfortunately, not all regions have

Balloter	Company	Seg-ment	Vote	Comment
				restoration plans, which is really the issue (which seems a violation to EOP-006-1 R3 to me).
Response: Thank you for your comments. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. The posted Guidance document has been modified to add reasoning for the threshold level. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				
Paul Shipps	Lakeland Electric	6	Negative	Avoid using "annual" - better to use "each calendar year" Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the regions black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). Better to say "Blackstart units and cranking paths determined as critical by the Reliability Coordinator"
Response: Thank you for your comments. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.				

Balloter	Company	Seg-ment	Vote	Comment
Randall McCamish	City of Vero Beach	1	Affirmative	The City of Vero Beach appreciates the hard work of the SDT. We have four issues that were not a big enough reason to vote Negative, but, we would like to see addressed: 1. Use of the word "annual". We would probably better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term. 2. 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the combined Contingency Reserves of entities within the Reliability Coordinator or something like that. 3. Automatic load shedding of 300 MW. The 300 MW is arbitrary and it ought to be any cyber-system controlled load shedding, not just automatic, of the same target of 1.1 (currently 1500 MW) 4. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the regions black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). The City of Vero Beach suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3.

Response: Thank you for your comments.

1. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.
2. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities.
3. The posted Guidance document has been modified to add reasoning for the threshold level.
4. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets.

Balloter	Company	Seg-ment	Vote	Comment
Ralph Frederick Meyer	Empire District Electric Co.	1	Negative	EDE appreciates the work that the drafting team has performed to get this standard to this point in the balloting process; however EDE casts a negative vote for the following reasons: 1) The term "annual" is used in R1 twice and R3 twice. While NERC has not defined the term annual I would suggest the drafting team take the approach to change the wording from "annual" to either "Twelve Full Calendar Months" or "Once per Calendar year". This would clarify two of these requirements in the proposed standard. By providing clarity hear avoids future conflicts between auditor's interpretations of this standard and the companies wishing to comply. 2) In attachment A, 1.4. EDE would suggest that the Drafting team change 1.4 to read: "Each Blackstart Unit identified in the Transmission Operator's Restoration Plan restoring the initial load to a group of generator units at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500MW." 3) And EDE would suggest the change to 1.5 to read: "The facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Unit identified in 1.4 to the first interconnection point of the generation unit(s) to be started, up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan." These thee changes would further signify the importance of the bright line on Highly Impact facilities to the Bulk Electric System that the drafting team is seeking to accomplish. We understand the effort the drafting team has put forth to this point and feel that they are close to a standard that the industry can comply with if some minor considerations were taken.

Response: Thank you for your comments.

1. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.
2. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to

Balloter	Company	Seg-ment	Vote	Comment
control frequency or voltage." Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. 3. Please refer to response to comment 2.				
Kenneth Simmons	Gainesville Regional Utilities	3	Affirmative	GRG has two comments we would liek to see addressed: 1- Attachment 1, bullets 1.4 and 1.5. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the region's black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). GRU suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3. 2- 2- Use of the word "annual". We would be better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term "annual"
Response: Thank you for your comments. 1. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. 2. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version.				
Matt Culverhouse	City of Bartow, Florida	3	Affirmative	FMPA appreciates the hard work of the SDT. We have four issues that were not a big enough reason to vote Negative, but, we would like to see addressed: 1. Use of the word "annual". We would probably better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term.

Balloter	Company	Seg-ment	Vote	Comment
				2. 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the combined Contingency Reserves of entities within the Reliability Coordinator or something like that 3. Automatic load shedding of 300 MW. The 300 MW is arbitrary and it ought to be any cyber-system controlled load shedding, not just automatic, of the same target of 1.1 (currently 1500 MW) 4. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the regions black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). FMPA suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3.
Response: Thank you for your comments. 1. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. 2. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. 3. The posted Guidance document has been modified to add reasoning for the threshold level. 4. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage."				
Stan T. Rzad	Keys Energy Services	1	Affirmative	Use of the word "annual", probably better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the contingency reserves of the Reliability Coordinator or something like that Automatic load shedding of 300 MW. The 300 MW is arbitrary and it ought to be any load shedding of the same target of 1.1 (currently 1500 MW) Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, not matter the importance to the region. This is not reasonable and only a few for the region ought to be identified (e.g., as identified in the regional plan). Unfortunately, not all regions have restoration plans, which is

Balloter	Company	Seg-ment	Vote	Comment
				really the issue (which seems a violation to EOP-006-1 R3 to me). FMPA appreciates the hard work of the SDT. We have five issues that were not a big enough reasons to vote Negative, but, we would like to see addressed: On Attachment 1, bullet 1.12, the phrase "for failure to operate as designed" was added since the last posting. We believe that this is inappropriate. Most SPS's are installed for automatic response to multi-contingency events. For an IROL to be exceeded, the multi-contingency event would need to occur at system conditions that would cause an IROL to be exceeded at the same time that the SPS failed to operate. The probability of the multi-contingency event occurring at such system conditions is very small (e.g., 1 in 50 year order of magnitude frequency), and the SPS would need to fail at that same time. We believe that the appropriate risk to protect against is manipulation of SPS at conditions experienced more frequently and we believe the original wording is correct.. Attachment 1, bullets 1.4 and 1.5. Any and all blackstart and cranking paths that are part of a TOP's restoration plan are included, no matter the importance to the region. This is not reasonable and only a few of the region's black-start unit and cranking paths ought to be identified as critical (e.g., as identified in the regional plan). FMPA suggests something like: "Blackstart units and cranking paths determined as critical by the Reliability Coordinator", which is similar in concept to Attachment 1, bullet 1.3. Use of the word "annual". We would probably be better off avoiding the word and saying something like "each calendar year but no longer than 16 months" to avoid controversy of the ambiguity of the term "annual". 1500 MW used in Attachment 1, item 1.1, and the 1000 MVAR used in 1.2, are rather arbitrary and ought to vary by region. 1.1 could use the combined Contingency Reserves of entities within the Reliability Coordinator or something like that Attachment 1, bullet 1.13 Automatic load shedding of 300 MW. The 300 MW is rather arbitrary and it ought to be any cyber-system controlled ability to shed load, not just automatic, of the same target of 1.1 (currently 1500 MW). Loss of 300 MW of load has less impact to BES reliability than loss of 300 MW of generation, so, there is inconsistency between the 1500 MW target for generation of bullet 1.1

Balloter	Company	Seg-ment	Vote	Comment
				and the 300 MW loss of load target of 1.13.
Response: Thank you for your comments. "Failure to operate as designed" was added to this criterion to account for human error, misconfigurations, improper change management (whether unintentional or malicious) The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions, regardless of MW capability. As such, these assets deserve protection as Critical Assets. The phraseology you are concerned about (annual) exists in the current CIP-002-3 standard. The SDT expects this phraseology to be resolved in the next version. The issue with using different MW values in each region is that it does not meet the objective of uniform application of Critical Asset identification across all entities. The posted Guidance document has been modified to add reasoning for the 300 MW threshold level.				
Allen Mosher	American Public Power Association	4	Abstain	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control

Balloter	Company	Seg-ment	Vote	Comment
				center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in redline CAPS/strikeout: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator[delete: 's restoration plan] SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or

Balloter	Company	Seg-ment	Vote	Comment
				low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)

Response: Thank you for your comment.
The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

Balloter	Company	Seg-ment	Vote	Comment
Nathan Mitchell	American Public Power Association	3	Abstain	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in redline CAPS/strikeout: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator's restoration plan SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for

Balloter	Company	Seg-ment	Vote	Comment
				full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.) If the SDT addresses this issue, APPA could recommend that the standard be approved.
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				

Balloter	Company	Seg-ment	Vote	Comment
Tony Eddleman	Nebraska Public Power District	3	Affirmative	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following to 1.4 and 1.5: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP

Balloter	Company	Seg-ment	Vote	Comment
				systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)

Response: Thank you for your comment.
The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

Balloter	Company	Seg-ment	Vote	Comment
John S Bos	Muscatine Power & Water	3	Negative	MP&W agrees with all APPA comments. APPA points out, there is an obvious consequence from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This noticeable interaction will cause many if not all registered TOP's, BA's, and GO's that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of the size of the entity. As the APPA points out, EOP-005 requires all TOPs to have a restoration plan. EOP-005 specifies that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a Critical Asset. Criterion 1.5 requires the identification of the Cranking Paths as Critical Assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a Critical Asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a Critical Asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, MP&W agrees with the APPA position in the following edits: Criterion 1.4. Each Blackstart Resource identified in the Restoration Plan for a Transmission Operator serving load or generation equal to or greater than an aggregate of 1500 MW in a single Interconnection. Criterion 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. MP&W agrees with surgical approach proposed by APPA, that ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full

Balloter	Company	Seg-ment	Vote	Comment
				CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." MP&W concurs with the APPA assessment that the experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES. Rather, their importance is to start generation to serve their small, local loads after a system separation. At this point, these smaller systems are to wait for direction from the Reliability Coordinator on resynchronization with the rest of the BES, once voltage and frequency are stabilized. MP&W again consents with the APPA comments. We recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Therefore, the revised criteria would support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				

Balloter	Company	Seg-ment	Vote	Comment
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Affirmative	The District believes to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. The District's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in redline CAPS/strikeout: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator's restoration plan SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009

Balloter	Company	Seg-ment	Vote	Comment
				compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
William G. Hutchison	Southern Illinois Power Coop.	1	Negative	SIPC believes there is an unintended consequence from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. EOP-005 requires all TOPs to

Balloter	Company	Seg-ment	Vote	Comment
				have a restoration plan. SIPC beleives that EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, the following edits to 1.4 and 1.5 are suggested. 1.4. Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than an aggregate of 1500 MW in a single Interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed “critical.” The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While it is recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)

Balloter	Company	Seg-ment	Vote	Comment
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Bob Essex	Cowlitz County PUD	5	Negative	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4

Balloter	Company	Seg-ment	Vote	Comment
				swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5: 1.4 Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than an aggregate of 1500 MW in a single interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4 to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their				

Balloter	Company	Seg-ment	Vote	Comment
availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Russell A Noble	Cowlitz County PUD	3	Negative	Please see comments submitted by Rick Syring of Cowlitz PUD. Cowlitz PUD commends the hard work of the SDT and hopes to change from a negative to an affirmative vote once the "catch 22" problem is fixed.
Response: Thank you for your comment.				
Bob C. Thomas	Illinois Municipal Electric Agency	4	Affirmative	IMEA appreciates the SDT's hard work to simplify and prioritize the CIP Reliability Standards by establishing reasonable brightline criteria. In addition to our Affirmative vote, IMEA supports the comments and concerns submitted by the American Public Power Association and the Florida Municipal Power Agency. We would support the proposed revisions as an improvement in clarity that will focus cyber security controls on assets that are truly critcial to BES real-time operations.
Response: Thank you for your comments. Please refer to the responses provided to APPA and the Florida Municipal Power Agency.				
Tim Kelley	Sacramento Municipal Utility District	1	Affirmative	SMUD supports the APPA comment noting that an approach that ensures generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical."
Mike Ramirez	Sacramento Municipal Utility District	4		
James Leigh-Kendall	Sacramento Municipal Utility	3		

Balloter	Company	Seg-ment	Vote	Comment
	District			
Bethany Hunter	Sacramento Municipal Utility District	5		
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Richard L. Koch	Nebraska Public Power District	1	Affirmative	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control

Balloter	Company	Seg-ment	Vote	Comment
				center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed “critical.” The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line

Balloter	Company	Seg-ment	Vote	Comment
				criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
James W. Beck	Transmission Agency of Northern California	1	Affirmative	"TANC supports the comments made by other APPA members regarding the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17."
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT				

Balloter	Company	Seg-ment	Vote	Comment
does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Danny Dees	MEAG Power	1	Affirmative	MEAG is sympathetic towards the position of the smaller APPA members (that are registered as a TOP) with regards to CIP 002-4 bringing into scope (as critical assets) smaller Blackstart Resources that may not necessarily be essential or critical to the operation of the BES.
Steven M. Jackson	Municipal Electric Authority of Georgia	3		
Steven Grego	MEAG Power	5		
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Linda R. Jacobson	City of Farmington	3	Affirmative	FEUS shares the concerns expressed by APPA with the draft standard regarding a 'catch 22' without a threshold designated for Blackstart Resources and cranking paths set forth in Criteria 1.4 and 1.5. However, FEUS believes the bright line criteria represented in CIP-002-4 is an improvement of the current CIP-002-3. FEUS also recognizes the importance of getting the bright line criteria approved; therefore, FEUS voted affirmative with an expectation the concern will be addressed in a future revision.
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their				

Balloter	Company	Seg-ment	Vote	Comment
availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Ernest Hahn	Metropolitan Water District of Southern California	1	Affirmative	Although MWD is voting yes, it supports the concern raised by the APPA CIP Task Force. The APPA Task Force has identified what may be an unintended consequence from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size.
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Jeff Knottek	City Utilities of	1	Negative	We support the comments submitted by the APPA task force.

Balloter	Company	Seg-ment	Vote	Comment
	Springfield, Missouri			
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Paul Morland	Colorado Springs Utilities	1	Affirmative	CSU shares the concerns expressed by many other APPA members with the draft standard and CSU would support the following proposed revision developed by the APPA CIP Task Force as an improvement in clarity that will focus cyber-security controls on assets that are truly Critical to BES real-time operations: The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires

Balloter	Company	Seg-ment	Vote	Comment
				each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in redline CAPS/strikeout: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator's restoration plan serving load or generation equal to or greater than an aggregate of 1500 MW in a single Interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through

Balloter	Company	Seg-ment	Vote	Comment
				development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
David Gordon	Massachusetts Municipal Wholesale Electric Company	5	Abstain	MMWEC shares APPA's concerns expressed with the draft standard. MMWEC would support APPA's proposed revision as an improvement in clarity that will focus cyber-security controls on assets that are truly Critical to BES real-time operations.
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these				

Balloter	Company	Seg-ment	Vote	Comment
resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Steve Alexanderson	Central Lincoln PUD	3	Abstain	Central Lincoln supports the following APPA CIP Task Force comments. If this issue is addressed as suggested, we will vote affirmative on the next ballot. The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through

Balloter	Company	Seg-ment	Vote	Comment
				1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in CAPS: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator SERVING LOAD OR GENERATION EQUAL TO OR GREATER THAN AN AGGREGATE OF 1500 MW IN A SINGLE INTERCONNECTION. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(S) IDENTIFIED IN 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their				

Balloter	Company	Seg-ment	Vote	Comment
availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				
Shamus J Gamache	Central Lincoln PUD	4	Abstain	Central Lincoln supports the following APPA CIP Task Force comments. If this issue is addressed as suggested, we will vote affirmative on the next ballot. The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-

Balloter	Company	Seg-ment	Vote	Comment
				002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5 shown in redline CAPS/strikeout: 1.4. Each Blackstart Resource identified in the RESTORATION PLAN FOR A Transmission Operator's restoration plan serving load or generation equal to or greater than an aggregate of 1500 MW in a single Interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4. to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical."
Response: Thank you for your comment. The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.				

Balloter	Company	Seg-ment	Vote	Comment
Rick Syring	Cowlitz County PUD	4	Negative	The APPA CIP Task Force has identified what we believe to be an unintended consequence – a Catch-22 – from the interaction of the revised CIP-002-4 Attachment 1's Criteria 1.4 (Blackstart Resources) and 1.5 (identified Cranking Paths) with the control center size and facility exceptions in 1.15, 1.16 and 1.17. This interaction will cause many if not all registered TOPs, BAs and Generation Owners that control Blackstart Resources used in a TOP restoration plan to become subject to CIP-002 through CIP-009, regardless of entity size. EOP-005 requires all TOPs to have a restoration plan. APPA's reading of EOP-005 indicates that each TOP must identify one or more Blackstart Resources. CIP-002-4 Criterion 1.4 requires a TOP to identify each such Blackstart Resource identified in its restoration plan as a critical asset. Criterion 1.5 requires the identification of certain Cranking Paths as critical assets. Criterion 1.15 requires that each generation control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for generation control center size (1500 MW). Criterion 1.16 requires each transmission control center or backup control center used to control a Cranking Path identified under Criterion 1.5 be identified as a critical asset, without any exception for TOP control center size. Criterion 1.17 requires each Balancing Authority control center or backup control center used to control a Blackstart Resource identified under Criterion 1.4 be identified as a critical asset, without any exception for Balancing Authority control center size (1500 MW). In effect, Criterion 1.4 swallows all exceptions created under 1.15 through 1.17, with the possible exception of a generation-only BA that does not have any Blackstart Resource obligations to its TOP. All vertically integrated utilities would be responsible for CIP-002 through CIP-009, including small BAs and TOPs that do not own any other Critical Assets. To address this problem, we propose the following edits to 1.4 and 1.5: 1.4. Each Blackstart Resource identified in the restoration plan for a Transmission Operator serving load or generation equal to or greater than an aggregate of 1500 MW in a single interconnection. 1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource(s) identified in 1.4 to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan. This surgical approach ensures that generation, TOP and BA control centers with responsibility for other critical generation and transmission assets are still responsible for full CIP-002-4 through CIP-009 compliance. However, small BA/TOP

Balloter	Company	Seg-ment	Vote	Comment
				systems with no initial obligations to the RC and larger TOPs for regional restoration would not be deemed "critical." The experience of these smaller systems is that their restoration obligations have not been relied upon to restore the BES, but rather to start generation to serve local load after a system separation – and then to wait for direction from the RC on resynchronization with the rest of the BES, once voltage and frequency are stabilized. While we recognize that cyber events may have an impact on the availability of resources, the fundamental fact is the vast majority of Blackstart Resources and control centers will be protected under CIP-002 through -009, because they will be classified as Critical/High Impact under the proposed criteria, as revised above. Thus the revised criteria support rather than undermine the distinction between categorization of big iron/big aluminum resources and their associated control centers as Critical or High Impact in the development of CIP-002-4. The categorization and development of security controls for smaller resources as either medium or low impact for the BES, should be addressed through development of additional bright line criteria and associated security controls in the next phase of this project (CIP-002-5 or CIP-010/011.)

Response: Thank you for your comment.
The SDT carefully selected criteria around the NERC Glossary term Blackstart Resource and its derivation from EOP-005-2. The team feels that these resources are critically important in their function to restore the BES under blackstart conditions. As such, these assets deserve protection as Critical Assets. Due to their connectivity and configuration, control centers that operate these Blackstart Resources also have the ability to jeopardize their availability and function in a time of need if maliciously misused. As such, these control centers should also be deemed Critical Assets. The SDT appreciates the "catch-22" concern that was brought forth by APPA. However, the SDT does not believe that the criteria as written present a catch-22 scenario. A careful reading of EOP-005-2 indicates that those assets identified as Blackstart Resources are those needed to bring the shutdown area "to a state whereby the choice of Load to be restored is not driven by the need to control frequency or voltage." The APPA comments indicate that the assets of concern to them are being utilized "once voltage and frequency are stabilized." As such, these assets are not required to be included in the TOP's restoration plan as Blackstart Resources. Additionally, it should be noted that EOP-005-2 does not presume that Blackstart Resources are only those "located within the Transmission Operator's System." As such, smaller TOPs have the opportunity to coordinate with neighboring TOPs and the RC in the development of their restoration plan which may not necessarily identify Blackstart Resources in their own system. In light of these clarifications, the SDT does not believe that a catch-22 exists that would unnecessarily bring in all TOP/BA control centers regardless of size, but rather only those that have the potential to impact Blackstart Resources that are essential to BES restoration as identified through EOP-005-2.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

NERC Cyber Security Standards Drafting Team for Order 706
December 2010

This document provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

TABLE OF CONTENTS

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION 3

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT 3

EXECUTIVE SUMMARY 3

INTRODUCTION 5

OVERALL APPLICATION OF ATTACHMENT 1 6

GENERATION 7

TRANSMISSION 12

CONTROL CENTERS 15

GUIDANCE ON THE IMPLEMENTATION PLAN 16

CONCLUSION 18

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

EXECUTIVE SUMMARY

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards and the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical

Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had

already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B, in the United States. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

OVERALL APPLICATION OF ATTACHMENT 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

GENERATION

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. Single plant location refers to a group of generating units occupying a defined physical footprint, often but not always, these units are surrounded by a common fence, have a common entry point, share common facilities such as warehouses, water plants and cooling sources, follow a similar naming convention (plant name - unit number) and fall under a common management organization. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system.

  In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES. In a

generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This may be illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility: in this case, the compromise of the cyber asset may result in an inability of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant time before this affects real-time operation, time during which detection and remediation may be able to be effected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are designated as Critical Assets. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where two or more path options exist as Critical Assets. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where two or more paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Special Protection Systems and Remedial Action Schemes may be implemented

to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Operators which own such systems and schemes must designate them as Critical Assets.

- Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets, or used to control generation greater than an aggregate of 1500 MW in a single Interconnection, as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections, and that BES impact will more likely be restricted within an Interconnection.

  This criterion uses the phrase "control generation." Entities should consider the discussion of "control" for generation as discussed in the Frequently Asked Questions (FAQ) document for CIP 002-1, Question 9:

  > **"Question:** *Are Cyber Assets for a control center or generation control center with monitoring only and no direct remote control required to be protected and secured under the Cyber Cyber Security Standards?*
  > **Answer:** A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.
  > An example of monitoring without direct control that is subject to the Cyber Security Standards is a Reliability Authority that receives data from Critical Cyber Assets to a state estimator. "

It must be noted that this part does not apply to those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document "Security Guideline for the Electric Sector: Identifying Critical Assets".

TRANSMISSION

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started". Part 1.5 specifies that the Facilities meeting these requirements or comprising the Cranking Paths be identified as Critical Assets.

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies,Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

  It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES: at this lower end of the EHV spectrum, the drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least 3 transmission stations or substations to ensure that the level of impact would be appropriate.

- Parts 1.8 and 1.9 include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits,** R5.1.1 and R5.1.3.

- Part 1.10 designates those Transmission Facilities as Critical Assets that provide the generation interconnection for Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates as Critical Assets those systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Critical Assets.

Within an operational environment the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold for inclusion as Critical Assets.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

CONTROL CENTERS

Parts 1.14 through 1.17 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation). While it is clear that the primary and all backup control centers operated by RCs, BAs, or TOPs **that meet the criteria** must be designated as Critical Assets, control centers at other applicable Responsible Entities that are used, by delegation, to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. It should be noted that Cyber Assets essential to the operation of a control center may be located at a data center that is not co-located with the control center itself.

- Part 1.14 designates all control centers used to perform the functional obligations of the Reliability Coordinator (RC) as Critical Assets. Each Reliability Coordinator control center and backup control center was included as a Critical Asset due to their key role in maintaining reliability for the Interconnection as a whole in concert with other Reliability Coordinators.

- For part 1.15, please refer to the discussion of generation control centers in the Generation section of this document.

- Part 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12. Due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. It must be noted that in many cases, some Transmission Operator functions are delegated to Transmission Owner control centers: in such cases, these must also be designated as Critical Assets. As with the discussion of part 1.15, the drafting team intended for the word control to have the same meaning as that found in *Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1* which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction."

- Part 1.17 specifies that all control centers that perform the functional obligations of the a Balancing Authority (BA) that include at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13 must be declared as Critical Assets. In addition, this criterion designates as a Critical Asset any BA control center that, in aggregate, performs the functional obligations of a BA for 1500 MWs or more in a single Interconnection. The threshold, controls generation of 1500 MW was chosen to maintain consistency with the threshold in part 1.1.

GUIDANCE ON THE IMPLEMENTATION PLAN

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. This implementation plan describes the schedule by which an Entity must become compliant with the Version 4 CIP Standards. Once this initial compliance milestone is reached, this implementation plan is effectively retired. For an Entity who registers after the Version 4 CIP

Standards are effective or for those Critical Cyber Assets that are newly identify after the Version 4 CIP Standards are effective, Responsible Entities should refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* The *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* remains in use throughout the entire time that the Version 4 CIP Standards remain in effect.

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date[3] specified in the Standard or (ii) the compliance milestones in the version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This allows essentially a two year implementation period following FERC approval to become compliant with the Version 4 CIP Standards. Special consideration was given to maintain the compliance milestone date for those Critical Cyber Assets and Newly Registered Entities that are in the middle of their implementation period for the Version 3 Standards on the Effective Date of the Version 4 Standards.

The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one-time implementation window was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-002-4 through CIP-009-4.

Both the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* contain certain exceptions for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.

[3] "The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)."

CONCLUSION

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

NERC Cyber Security Standards Drafting Team for Order 706
~~September~~ December 2010

This document provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

TABLE OF CONTENTS

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION 3

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT 3

EXECUTIVE SUMMARY 3

INTRODUCTION 5

OVERALL APPLICATION OF ATTACHMENT 1 6

GENERATION 7

TRANSMISSION 12

CONTROL CENTERS 15

GUIDANCE ON THE IMPLEMENTATION PLAN 16

CONCLUSION 18

CIP-002-4 – CYBER SECURITY - CRITICAL CYBER ASSET IDENTIFICATION

RATIONALE AND IMPLEMENTATION REFERENCE DOCUMENT

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

EXECUTIVE SUMMARY

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards and the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical

Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had

already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B, in the United States. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

OVERALL APPLICATION OF ATTACHMENT 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it leaves some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

GENERATION

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. Single plant location refers to a group of generating units occupying a defined physical footprint, often but not always, these units are surrounded by a common fence, have a common entry point, share common facilities such as warehouses, water plants and cooling sources, follow a similar naming convention (plant name - unit number) and fall under a common management organization. The 1500 MW~~This~~ criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system.

  In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES. In a

generation facility context, there may be Facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes. This may be illustrated in the case of cyber assets controlling the supply of coal fuel in a coal burning facility: in this case, the compromise of the cyber asset may result in an inability of the supply system to bring the fuel for generation. However, because of the way these systems are used, there may be a significant time before this affects real-time operation, time during which detection and remediation may be able to be effected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as necessary to avoid BES Adverse Reliability Impacts in the long term planning horizon are designated as Critical Assets. These Facilities may be designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  In the specification of the "long-term planning horizon" in this criterion, the drafting team sought to ensure that such Critical Assets would be designated in the time horizon described in the NERC document "Time Horizons", which defines long-term planning horizon as "a planning horizon of one year or longer".

If it is determined through system studies that a unit must run in order to preserve the reliability of the BES, such as due to a category C3 contingency as defined in TPL-003 or a category D contingency as defined in TPL-004, then that unit must be classified as a Critical Asset.

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where two or more path options exist as Critical Assets. This criterion is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where two or more paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Special Protection Systems and Remedial Action Schemes may be implemented

to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Operators which ~~have implemented~~own such systems and schemes must designate them as Critical Assets.

- Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets, or used to control generation greater than an aggregate of 1500 MW in a single Interconnection, as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections, and that BES impact will more likely be restricted within an Interconnection.

  This criterion uses the phrase "control generation." Entities should consider the discussion of "control" for generation as discussed in the Frequently Asked Questions (FAQ) document for CIP 002-1, Question 9:

  > **"Question:** *Are Cyber Assets for a control center or generation control center with monitoring only and no direct remote control required to be protected and secured under the Cyber Cyber Security Standards?*
  > **Answer:** A control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.
  > An example of monitoring without direct control that is subject to the Cyber Security Standards is a Reliability Authority that receives data from Critical Cyber Assets to a state estimator. "

It must be noted that this part does not apply to those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document "Security Guideline for the Electric Sector: Identifying Critical Assets".

TRANSMISSION

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the "Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started". Part 1.5 specifies that the Facilities meeting these requirements or comprising the Cranking Paths be identified as Critical Assets.

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies,Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

  It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for EHV Transmission Facilities, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES: at this lower end of the EHV spectrum, the drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least 3 transmission stations or substations to ensure that the level of impact would be appropriate.

- Parts 1.8 and 1.9 include those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits,** R5.1.1 and R5.1.3.

- Part 1.10 designates those Transmission Facilities as Critical Assets that provide the generation interconnection for Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these Critical Assets would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates as Critical Assets those systems or Facilities that are capable of performing automatic load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of criterion 1.13, and chose the term "Each" to represent that the criterion applied to a discrete system or Facility. In the drafting of this criterion, the drafting team sought to include only those systems that did not require human operator initiation, and targeted in particular those Under Frequency Load Shedding (UFLS) facilities and systems and Under Voltage Load Shedding (UVLS) facilities and systems that would be implemented as part of a regional load shedding requirement to prevent Adverse Reliability Impact. These include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as Critical Assets.

Within an operational environment the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with loss of load resulting in a frequency high condition and a loss of generation resulting in a frequency low condition. This particular threshold (300 MW) was provided in CIP version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold for inclusion as Critical Assets.~~300 MW is the reporting threshold for DOE EIA-417.~~

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market.

CONTROL CENTERS

Parts 1.14 through 1.17 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for only a single BES asset should be evaluated as part of the BES asset (e.g., control room for a single generation plant or transmission substation). While it is clear that the primary and all backup control centers operated by RCs, BAs, or TOPs **that meet the criteria** must be designated as Critical Assets, control centers at other applicable Responsible Entities that are used, by delegation, to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. It should be noted that Cyber Assets essential to the operation of a control center may be located at a data center that is not co-located with the control center itself.

- Part 1.14 designates all control centers used to perform the functional obligations of the Reliability Coordinator (RC) as Critical Assets. Each Reliability Coordinator control center and backup control center was included as a Critical Asset due to their key role in maintaining reliability for the Interconnection as a whole in concert with other Reliability Coordinators.

- For part 1.15, please refer to the discussion of generation control centers in the Generation section of this document.

- Part 1.16 specifies that all control centers or backup control centers that perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12. Due to the direct impact on the operation of identified Critical Assets, these Transmission control centers must be designated as Critical Assets. It must be noted that in many cases, some Transmission Operator functions are delegated to Transmission Owner control centers: in such cases, these must also be designated as Critical Assets. As with the discussion of part 1.15, the drafting team intended for the word control to have the same meaning as that found in *Frequently Asked Questions Cyber Security Standards CIP-002-1 through CIP-009-1* which indicates that controls may be "performed automatically, remotely, manually, or by voice instruction."

- Part 1.17 specifies that all control centers that perform the functional obligations of the a Balancing Authority (BA) that include at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13 must be declared as Critical Assets. In addition, this criterion designates as a Critical Asset any BA control center that, in aggregate, performs the functional obligations of a BA for 1500 MWs or more in a single Interconnection. The threshold, controls generation of 1500 MW was chosen to maintain consistency with the threshold in part 1.1.

GUIDANCE ON THE IMPLEMENTATION PLAN

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. This implementation plan describes the schedule by which an Entity must become compliant with the Version 4 CIP Standards. Once this initial compliance milestone is reached, this implementation plan is effectively retired. For an Entity who registers after the Version 4 CIP

Standards are effective or for those Critical Cyber Assets that are newly identify after the Version 4 CIP Standards are effective, Responsible Entities should refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* The *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* remains in use throughout the entire time that the Version 4 CIP Standards remain in effect.

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date[3] specified in the Standard or (ii) the compliance milestones in the version 3 Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This allows essentially a two year implementation period following FERC approval to become compliant with the Version 4 CIP Standards. Special consideration was given to maintain the compliance milestone date for those Critical Cyber Assets and Newly Registered Entities that are in the middle of their implementation period for the Version 3 Standards on the Effective Date of the Version 4 Standards.

The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one-time implementation window was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-002-4 through CIP-009-4.

Both the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4* and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* contain certain exceptions for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.

[3] "The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)."

CONCLUSION

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by*

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

the Responsible Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

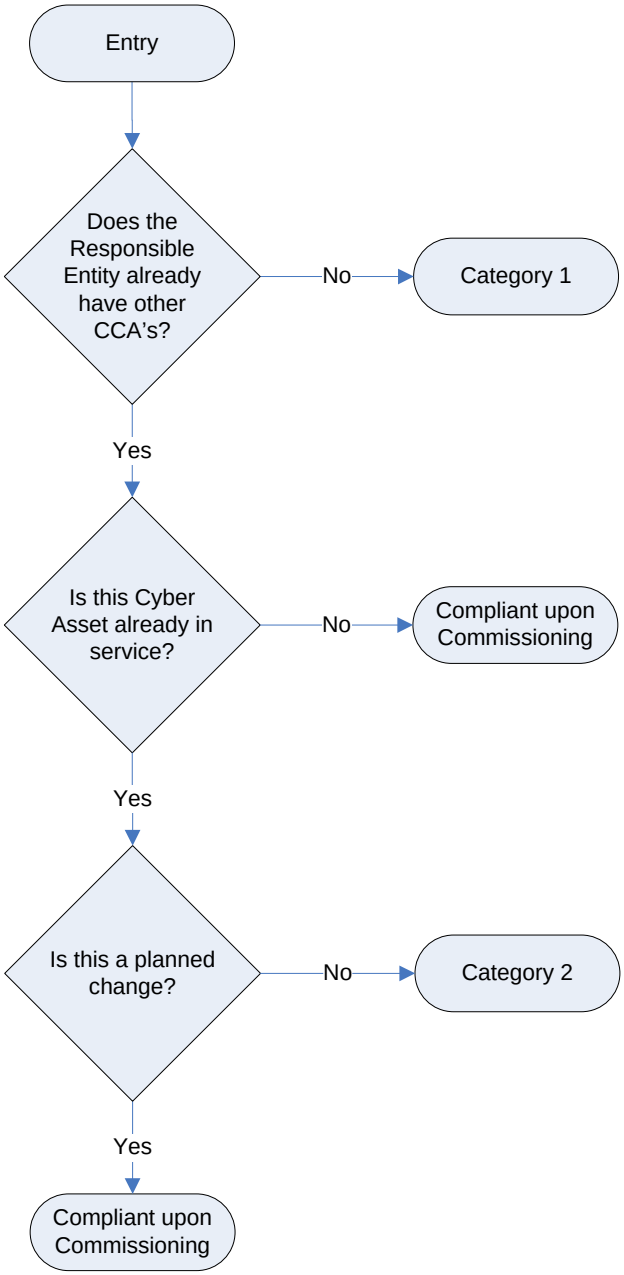


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In

this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the access authorization process.

The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merged plan is being performed. Progress towards meeting milestones and completing the merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly identified Critical Asset, but no newly identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon identification of a Critical Asset without associated Critical Cyber Assets. Only upon identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets[4]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

[4] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5][6] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	**Registration + 12 months**	**Registration + 24 months**
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.
[6] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The effective date of EOP-005-2 is the date that Criteria 1.4 and 1.5 will be used to determine Critical Assets for Responsible Entity.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority
• Interchange Authority
• Transmission Service Provider
• Transmission Owner
• Transmission Operator
• Generator Owner
• Generator Operator
• Load Serving Entity
• NERC
• Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities

For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4, (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage, or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The effective date of EOP-005-2 is the date that ~~definition must be approved before~~ Criteria 1.4 and 1.5 ~~are~~ will be used to determine Critical Assets for Responsible ~~Entities~~Entity.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority
• Interchange Authority
• Transmission Service Provider
• Transmission Owner
• Transmission Operator
• Generator Owner
• Generator Operator

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities

Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities

For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4, (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage, or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Recirculation Ballot Window Opens December 20-30, 2010

Now available at: https://standards.nerc.net/CurrentBallots.aspx

Project 2008-06: Cyber Security Order 706

A recirculation ballot window for standard CIP-002-4 — Critical Cyber Asset Identification is open **until 8 p.m. Eastern on Thursday, December 30th, 2010**.

Instructions

Members of the ballot pools associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

Ballot Process

The Standards Committee encourages all members of the ballot pool to review the consideration of comments submitted during the last ballot window. In the recirculation ballot, votes are counted by exception only — if a ballot pool member does not submit a revision to that member's original vote, the vote remains the same as in the first ballot. Members of the ballot pool may:

- Reconsider and change their votes from the first ballot
- Vote in the second ballot even if they did not vote on the first ballot
- Take no action if they do not want to change their original vote

Additional Information

The Standard Processes Manual allows drafting teams to make changes following an initial or successive ballot with a goal of improving the quality of a standard, provided those changes do not alter the applicability or scope of the proposed standard. Following the initial ballot, the Project 2008-06 drafting team made minor changes to CIP-002-4 and the associated guidance document and implementation plan. Redlines against the last posted documents as well as the last approved versions of CIP-002 through CIP-009, along with redlines of the guidance document and implementation plan against the last posted versions have been posted on the project page for stakeholder review.

Next Steps

Voting results will be posted and announced after the ballot window closes. If approved, the standard, Violation Risk Factors and Violation Severity Levels, guidance document, and associated implementation plan will be submitted to the Board of Trustees.

Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with

the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

The team has been working to revise CIP-002 – Identification of Critical Assets, with the goal of establishing bright line criteria for the identification of critical assets. In November, the SC Executive Committee authorized the team to conduct an abbreviated comment period in parallel with a successive ballot, to support providing stakeholders with the opportunity to provide comment, while also supporting the goal of completing this set of revisions to CIP-002 before the end of December, 2010.

Applicability of Standards in Project

Reliability Coordinator
Balancing Authority
Interchange Authority
Transmission Service Provider
Transmission Owner
Transmission Operator
Generator Owner
Generator Operator
Load-Serving Entity
NERC
Regional Entity

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 609.452.8060.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

User Name
Password
Log in
Register

-Ballot Pools
-Current Ballots
-Ballot Results
-Registered Ballot Body
-Proxy Voters

Home Page

Ballot Results

Ballot Name:	Project 2008-06 Cyber Security 706 (Version 4 CIP Standards)_sb_rc
Ballot Period:	12/20/2010 - 12/30/2010
Ballot Type:	recirculation
Total # Votes:	371
Total Ballot Pool:	410
Quorum:	**90.49 % The Quorum has been reached**
Weighted Segment Vote:	80.56 %
Ballot Results:	**The Standard has Passed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Abstain # Votes	No Vote
1 - Segment 1.	113	1	91	0.85	16	0.15	2	4
2 - Segment 2.	11	0.8	3	0.3	5	0.5	3	0
3 - Segment 3.	93	1	72	0.911	7	0.089	3	11
4 - Segment 4.	30	1	23	0.92	2	0.08	4	1
5 - Segment 5.	87	1	58	0.829	12	0.171	5	12
6 - Segment 6.	51	1	35	0.854	6	0.146	3	7
7 - Segment 7.	1	0	0	0	0	0	0	1
8 - Segment 8.	10	0.8	4	0.4	4	0.4	0	2
9 - Segment 9.	5	0.4	4	0.4	0	0	0	1
10 - Segment 10.	9	0.9	9	0.9	0	0	0	0
Totals	**410**	**7.9**	**299**	**6.364**	**52**	**1.536**	**20**	**39**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	Comments
1	Allegheny Power	Rodney Phillips	Affirmative	
1	Ameren Services	Kirit S. Shah	Affirmative	View
1	American Electric Power	Paul B. Johnson	Affirmative	View
1	American Transmission Company, LLC	Jason Shaver	Affirmative	View
1	Arizona Public Service Co.	Robert D Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	Avista Corp.	Scott Kinney	Affirmative	
1	Baltimore Gas & Electric Company	Gregory S Miller	Affirmative	View

1	BC Transmission Corporation	Gordon Rawlings	Affirmative	View
1	Beaches Energy Services	Joseph S. Stonecipher	Affirmative	
1	Black Hills Corp	Eric Egge	Affirmative	
1	Bonneville Power Administration	Donald S. Watkins	Negative	View
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Negative	View
1	CenterPoint Energy	Paul Rocha	Negative	View
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Maine Power Company	Brian Conroy		
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Vero Beach	Randall McCamish	Affirmative	View
1	City Utilities of Springfield, Missouri	Jeff Knottek	Affirmative	View
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Paul Morland	Affirmative	View
1	Commonwealth Edison Co.	Gregory Campbell		
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	Dayton Power & Light Co.	Hertzel Shamash	Affirmative	
1	Deseret Power	James Tucker	Affirmative	
1	Dominion Virginia Power	John K Loftis	Affirmative	
1	Duke Energy Carolina	Douglas E. Hils	Affirmative	
1	E.ON U.S.	Larry Monday		
1	East Kentucky Power Coop.	George S. Carruba	Affirmative	
1	Edison Electric Institute	David Batz	Affirmative	View
1	Empire District Electric Co.	Ralph Frederick Meyer	Negative	View
1	Entergy Corporation	George R. Bartlett	Affirmative	
1	FirstEnergy Energy Delivery	Robert Martinko	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	GDS Associates, Inc.	Claudiu Cadar	Abstain	
1	Georgia Transmission Corporation	Harold Taylor, II	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Robert Solomon	Affirmative	
1	Hydro One Networks, Inc.	Ajay Garg	Negative	View
1	Hydro-Quebec TransEnergie	Bernard Pelletier	Negative	View
1	Idaho Power Company	Ronald D. Schellberg	Affirmative	
1	Indianapolis Power & Light Co.	Michael Holtsclaw	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Affirmative	View
1	JEA	Ted E Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Michael Gammon	Affirmative	View
1	Keys Energy Services	Stan T. Rzad	Affirmative	View
1	Lake Worth Utilities	Walt Gill	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John W Delucca	Negative	View
1	Lincoln Electric System	Doug Bantam		
1	Long Island Power Authority	Robert Ganley	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	View
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Joe D Petaski	Affirmative	
1	MEAG Power	Danny Dees	Affirmative	View
1	Metropolitan Water District of Southern California	Ernest Hahn	Affirmative	View
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi Woodward	Affirmative	
1	Minnkota Power Coop. Inc.	Richard Burt	Negative	View
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid	Saurabh Saksena	Affirmative	
1	Nebraska Public Power District	Richard L. Koch	Affirmative	View
1	Nevada Power Co.	James McMorran	Negative	View
1	New York Power Authority	Arnold J. Schuff	Negative	
1	North Carolina Electric Membership Corp.	Gary Ofner	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	David H. Boguslawski	Affirmative	
1	Northern Indiana Public Service Co.	Kevin M Largura	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Robert Mattey	Negative	

1	Oklahoma Gas and Electric Co.	Marvin E VanBebber	Affirmative	
1	Omaha Public Power District	Douglas G Peterchuck	Affirmative	
1	Oncor Electric Delivery	Michael T. Quinn	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Chifong L. Thomas	Affirmative	
1	PacifiCorp	Colt Norrish	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	Frank F. Afranji	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PowerSouth Energy Cooperative	Larry D. Avery	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	View
1	Progress Energy Carolinas	Sammy Roberts	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Puget Sound Energy, Inc.	Catherine Koch	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	View
1	Salt River Project	Robert Kondziolka	Affirmative	
1	Santee Cooper	Terry L. Blackwell	Affirmative	
1	SCE&G	Henry Delk, Jr.	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	View
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Sierra Pacific Power Co.	Rich Salgo	Negative	View
1	South Texas Electric Cooperative	Richard McLeon	Affirmative	
1	Southern California Edison Co.	Dana Cabbell	Affirmative	
1	Southern Company Services, Inc.	Horace Stephen Williamson	Affirmative	View
1	Southern Illinois Power Coop.	William G. Hutchison	Negative	View
1	Southwest Transmission Cooperative, Inc.	James L. Jones	Affirmative	View
1	Southwestern Power Administration	Gary W Cox	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Larry Akens	Abstain	
1	Transmission Agency of Northern California	James W. Beck	Affirmative	View
1	Tri-State G & T Association, Inc.	Keith V. Carman	Affirmative	
1	Tucson Electric Power Co.	John Tolo	Negative	View
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Brandy A Dunn	Negative	View
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	Alberta Electric System Operator	Mark B Thompson	Abstain	
2	BC Hydro	Venkataramakrishnan Vinnakota	Affirmative	
2	California ISO	Gregory Van Pelt	Abstain	
2	Electric Reliability Council of Texas, Inc.	Chuck B Manning	Negative	View
2	Independent Electricity System Operator	Kim Warren	Negative	View
2	ISO New England, Inc.	Kathleen Goodman	Negative	View
2	Midwest ISO, Inc.	Jason L Marshall	Negative	View
2	New Brunswick System Operator	Alden Briggs	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Abstain	
2	PJM Interconnection, L.L.C.	Tom Bowe	Affirmative	
2	Southwest Power Pool	Charles H Yeung	Negative	View
3	Alabama Power Company	Richard J. Mandes	Affirmative	View
3	Allegheny Power	Bob Reeping	Affirmative	
3	Ameren Services	Mark Peters	Affirmative	
3	American Electric Power	Raj Rana		
3	American Public Power Association	Nathan Mitchell	Affirmative	View
3	Anaheim Public Utilities Dept.	Kelly Nguyen		
3	APS	Steven Norris	Affirmative	
3	Associated Electric Cooperative, Inc.	Chris W Bolick	Affirmative	
3	Atlantic City Electric Company	James V. Petrella	Affirmative	
3	Avista Corp.	Robert Lafferty	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Affirmative	
3	Blue Ridge Power Agency	Duane S Dahlquist		
3	Bonneville Power Administration	Rebecca Berdahl	Negative	View
3	Central Electric Power Cooperative	Ralph J Schulte		

3	Central Lincoln PUD	Steve Alexanderson	Abstain	View
3	City of Bartow, Florida	Matt Culverhouse	Affirmative	View
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R. Jacobson	Affirmative	View
3	City of Green Cove Springs	Gregg R Griffin	Affirmative	View
3	City of Leesburg	Phil Janik		
3	City Water, Light & Power of Springfield	Roger Powers		
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	ComEd	Bruce Krawczyk	Affirmative	View
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy	David A. Lapinski	Negative	View
3	Cowlitz County PUD	Russell A Noble	Affirmative	View
3	CPS Energy	Edwin Les Barrow		
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Detroit Edison Company	Kent Kujala	Affirmative	
3	Dominion Resources Services	Michael F Gildea	Affirmative	
3	Duke Energy Carolina	Henry Ernst-Jr	Affirmative	View
3	East Kentucky Power Coop.	Sally Witt	Affirmative	
3	Entergy	Joel T Plessinger	Affirmative	
3	FirstEnergy Solutions	Kevin Querry	Affirmative	
3	Flathead Electric Cooperative	John M Goroski	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney		
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	View
3	Georgia Power Company	Anthony L Wilson	Affirmative	View
3	Georgia System Operations Corporation	R Scott S. Barfield-McGinnis	Affirmative	
3	Great River Energy	Sam Kokkinen	Affirmative	
3	Gulf Power Company	Gwen S Frazier		
3	Hydro One Networks, Inc.	David L Kiguel	Negative	View
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes	Affirmative	
3	Kansas City Board of Public Utilities	Robert D Adam	Affirmative	View
3	Kansas City Power & Light Co.	Charles Locke	Affirmative	View
3	Kissimmee Utility Authority	Gregory David Woessner	Affirmative	
3	Lakeland Electric	Mace Hunter	Affirmative	
3	Lincoln Electric System	Bruce Merrill	Negative	View
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	View
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Madison Gas and Electric Co.	Darl Shimko	Abstain	View
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Mississippi Power	Don Horsley	Affirmative	View
3	Municipal Electric Authority of Georgia	Steven M. Jackson	Affirmative	View
3	Muscatine Power & Water	John S Bos	Negative	View
3	Nebraska Public Power District	Tony Eddleman	Affirmative	View
3	New York Power Authority	Marilyn Brown	Affirmative	
3	Niagara Mohawk (National Grid Company)	Michael Schiavone		
3	North Carolina Municipal Power Agency #1	Denise Roeder	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	William SeDoris	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Negative	View
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Electric Utility	David T. Anderson	Affirmative	
3	Orange and Rockland Utilities, Inc.	David Burke	Affirmative	
3	Orlando Utilities Commission	Ballard Keith Mutters	Affirmative	
3	Owensboro Municipal Utilities	Richard H. Chapman		
3	PacifiCorp	John Apperson	Affirmative	
3	PECO Energy an Exelon Co.	Vincent J. Catania	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Potomac Electric Power Co.	Robert Reuter	Affirmative	
3	Progress Energy Carolinas	Sam Waters	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 2 of Grant County	Greg Lange	Affirmative	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	View
3	Salt River Project	John T. Underhill	Affirmative	
3	San Diego Gas & Electric	Scott Peterson	Negative	View

3	Santee Cooper	Zack Dusenbury	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	View
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C. Young	Affirmative	
3	Southern California Edison Co.	David Schiada	Affirmative	
3	Tacoma Public Utilities	Travis Metcalfe	Affirmative	
3	Tampa Electric Co.	Ronald L Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State G & T Association, Inc.	Janelle Marriott	Affirmative	
3	Wisconsin Electric Power Marketing	James R. Keller	Affirmative	View
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	American Municipal Power - Ohio	Kevin Koloini	Abstain	
4	American Public Power Association	Allen Mosher	Affirmative	View
4	Central Lincoln PUD	Shamus J Gamache	Abstain	View
4	City of Clewiston	Kevin McCarthy	Affirmative	
4	City of New Smyrna Beach Utilities Commission	Timothy Beyrle	Affirmative	View
4	Consumers Energy	David Frank Ronk	Negative	View
4	Cowlitz County PUD	Rick Syring	Affirmative	View
4	Detroit Edison Company	Daniel Herring	Affirmative	
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	View
4	Fort Pierce Utilities Authority	Thomas W. Richards	Affirmative	
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	View
4	Indiana Municipal Power Agency	Jack Alvey	Affirmative	View
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	View
4	LaGen	Richard Comeaux	Negative	View
4	Madison Gas and Electric Co.	Joseph G. DePoorter	Abstain	View
4	National Rural Electric Cooperative Association	Barry Lawson	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Terri Pyle	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Abstain	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean	Affirmative	
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen	Affirmative	View
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	View
4	Seattle City Light	Hao Li	Affirmative	View
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	View
4	Wisconsin Public Power Inc.	Patrick Connors	Affirmative	
5	AEP Service Corp.	Brock Ondayko	Affirmative	View
5	Allegheny Energy Supply Company, LLC	Robert Loy	Negative	
5	Amerenue	Sam Dwyer	Affirmative	
5	APS	Mel Jensen	Affirmative	
5	Associated Electric Cooperative, Inc.	Brad Haralson		
5	Avista Corp.	Edward F. Groce	Affirmative	
5	BC Hydro and Power Authority	Clement Ma		
5	Black Hills Corp	George Tatar	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Negative	View
5	Chelan County Public Utility District #1	John Yale	Affirmative	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Grand Island	Jeff Mead	Negative	View
5	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Max Emrick	Affirmative	
5	City of Tallahassee	Alan Gale	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Consolidated Edison Co. of New York	Wilket (Jack) Ng	Affirmative	
5	Constellation Power Source Generation, Inc.	Amir Y Hammad	Affirmative	View
5	Consumers Energy	James B Lewis	Negative	View
5	Cowlitz County PUD	Bob Essex	Affirmative	View
5	CPS Energy	Robert B Stevens	Affirmative	
5	Detroit Edison Company	Christy Wicke	Affirmative	
5	Dominion Resources, Inc.	Mike Garton	Affirmative	

5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	East Kentucky Power Coop.	Stephen Ricker	Affirmative	
5	Energy Northwest - Columbia Generating Station	Doug Ramey	Affirmative	
5	Entergy Corporation	Stanley M Jaskot	Affirmative	
5	ExxonMobil Research and Engineering	Martin Kaufman	Negative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	View
5	Florida Municipal Power Agency	David Schumann	Affirmative	View
5	Great River Energy	Cynthia E Sulzer	Affirmative	
5	Green Country Energy	Greg Froehling	Affirmative	
5	Horizon Wind Energy	Brent Hebert	Negative	View
5	Indeck Energy Services, Inc.	Rex A Roehl	Affirmative	
5	Kansas City Power & Light Co.	Scott Heidtbrink	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lakeland Electric	Thomas J Trickey		
5	Liberty Electric Power LLC	Daniel Duff	Negative	
5	Lincoln Electric System	Dennis Florom	Negative	View
5	Louisville Gas and Electric Co.	Charlie Martin		
5	Lower Colorado River Authority	Tom Foreman	Affirmative	
5	Luminant Generation Company LLC	Mike Laney	Affirmative	View
5	Madison Gas and Electric Co.	Steven Schultz	Abstain	View
5	Manitoba Hydro	S N Fernando	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	View
5	MEAG Power	Steven Grego	Affirmative	View
5	Michigan Public Power Agency	James R. Nickel		
5	MidAmerican Energy Co.	Christopher Schneider	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	View
5	New York Power Authority	Gerald Mannarino	Negative	
5	Northern Indiana Public Service Co.	Michael K Wilkerson	Affirmative	
5	NRG Energy, Inc.	Patricia A. Lynch	Negative	View
5	Occidental Chemical	Michelle DAntuono	Affirmative	View
5	Oglethorpe Power Corporation	Scott McGough	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	Colin Anderson	Affirmative	
5	Orlando Utilities Commission	Richard Kinas		
5	Pacific Gas and Electric Company	Richard J. Padilla	Affirmative	
5	PacifiCorp	Sandra L. Shaffer	Affirmative	
5	Portland General Electric Co.	Gary L Tingley	Affirmative	
5	PowerSouth Energy Cooperative	Tim Hattaway	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	Progress Energy Carolinas	Wayne Lewis	Affirmative	
5	PSEG Power LLC	Jerzy A Slusarz	Affirmative	
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Reedy Creek Energy Services	Bernie Budnik		
5	RRI Energy	Thomas J. Bradish	Abstain	
5	Sacramento Municipal Utility District	Bethany Hunter	Affirmative	View
5	Salt River Project	Glen Reeves	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	View
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins	Affirmative	
5	South Carolina Electric & Gas Co.	Richard Jones		
5	South Mississippi Electric Power Association	Jerry W Johnson		
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	George T. Ballew	Abstain	
5	Trans Canada Power	John Fish		
5	TransAlta Centralia Generation, LLC	Joanna Luong-Tran	Abstain	View
5	Tri-State G & T Association, Inc.	Barry Ingold	Affirmative	
5	U.S. Army Corps of Engineers	Melissa Kurtz	Negative	View
5	U.S. Bureau of Reclamation	Martin Bauer P.E.	Affirmative	
5	US Power Generating Company	Bohdan M Dackow	Negative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	View
5	Wisconsin Public Service Corp.	Leonard Rentmeester		
5	Xcel Energy, Inc.	Liam Noailles	Affirmative	

6	AEP Marketing	Edward P. Cox	Affirmative	View
6	Ameren Energy Marketing Co.	Jennifer Richardson	Affirmative	View
6	Arizona Public Service Co.	Justin Thompson	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Negative	View
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Consolidated Edison Co. of New York	Nickesha P Carrol	Affirmative	
6	Constellation Energy Commodities Group	Brenda Powell	Negative	View
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy Carolina	Walter Yeager	Negative	
6	Entegra Power Services	Larry W. Rodriguez	Negative	View
6	Entergy Services, Inc.	Terri F Benoit	Affirmative	
6	Exelon Power Team	Pulin Shah	Affirmative	
6	FirstEnergy Solutions	Mark S Travaglianti	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	View
6	Florida Municipal Power Pool	Thomas E Washburn	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	View
6	Lakeland Electric	Paul Shipps	Affirmative	View
6	Lincoln Electric System	Eric Ruskamp	Negative	View
6	Louisville Gas and Electric Co.	Daryn Barker		
6	Luminant Energy	Brad Jones	Affirmative	View
6	Madison Gas and Electric Co.	Jeffrey M Keebler	Abstain	View
6	Manitoba Hydro	Daniel Prowse	Affirmative	
6	MidAmerican Energy Co.	Dennis Kimm	Affirmative	
6	Missouri River Energy Services	Gerald A. Tielke		
6	North Carolina Municipal Power Agency #1	Matthew Schull		
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	View
6	NRG Energy, Inc.	Alan R. Johnson	Negative	
6	Omaha Public Power District	David Ried	Affirmative	
6	Orlando Utilities Commission	Claston Augustus Sunanon	Affirmative	
6	PacifiCorp	Scott L Smith	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	John Jamieson	Affirmative	
6	PPL EnergyPlus LLC	Mark A Heimbach	Abstain	
6	Progress Energy	John T Sturgeon	Affirmative	
6	PSEG Energy Resources & Trade LLC	James D. Hebson	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	RRI Energy	Trent Carlson		
6	Salt River Project	Mike Hummel	Affirmative	
6	Santee Cooper	Suzanne Ritter	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	SunGard Data Systems	Christopher K Heisler		
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Western Area Power Administration - UGP Marketing	John Stonebarger		
6	Wisconsin Public Service Corp.	Paul Spicer		
6	Xcel Energy, Inc.	David F. Lemmons	Affirmative	
7	Oak Ridge National Laboratory	Stacy Prowell		
8		John Kutzer		
8		Scott Hudson		
8		James A Maenner	Negative	
8		Roger C Zaklukiewicz	Affirmative	
8		Edward C Stein	Affirmative	
8	JDRJC Associates	Jim D. Cyrulewski	Negative	
8	Network & Security Technologies	Nicholas Lauriat	Affirmative	
8	SPS Consulting Group Inc.	Jim R Stanton	Negative	View
8	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	California Energy Commission	William Mitchell Chamberlain	Affirmative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald E. Nelson	Affirmative	
9	North Carolina Utilities Commission	Kimberly J. Jones		

9	Oregon Public Utility Commission	Jerome Murray	Affirmative	
9	Utah Public Service Commission	Ric Campbell	Affirmative	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	James D Burley	Affirmative	
10	New York State Reliability Council	Alan Adamson	Affirmative	
10	Northeast Power Coordinating Council, Inc.	Guy V. Zito	Affirmative	View
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Carter B Edge	Affirmative	View
10	Southwest Power Pool Regional Entity	Stacy Dochoda	Affirmative	View
10	Texas Reliability Entity	Larry D. Grimm	Affirmative	View
10	Western Electricity Coordinating Council	Louise McCarren	Affirmative	View

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
Washington Office: 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement
Recirculation Ballot Results

Now available at: https://standards.nerc.net/Ballots.aspx

Ballot Results for Project 2008-6: CIP-002-4 Critical Asset Identification

The recirculation ballot window to vote on proposed revisions to CIP-002 closed on December 30, 2010. The ballot pool has approved the following standards and associated implementation plans:

CIP–002–4—Cyber Security — Critical Cyber Asset Identification
CIP–003–4— Cyber Security — Security Management Controls
CIP–004–4— Cyber Security — Personnel and Training
CIP–005–4— Cyber Security — Electronic Security Perimeter(s)
CIP–006–4— Cyber Security — Physical Security
CIP–007–4—Cyber Security — Systems Security Management
CIP–008–4—Cyber Security — Incident Reporting and Response Planning
CIP–009–4— Cyber Security — Recovery Plans for Critical Cyber Assets

Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results.

Quorum: 90.49%
Approval: 80.56%

Background

FERC Order 706 directed NERC to develop modifications to the CIP Reliability Standards. Due to the variety of changes directed in Order 706 and the complexity of the project, the drafting team adopted a multi-phase revision strategy. The initial phase involved modifying standards CIP-002-1 through CIP-009-1 to comply with the near-term directives included in Order 706. The resulting version 2 CIP standards were approved by the NERC Board of Trustees, and as part of its approval Order, FERC directed NERC to make changes to two standards and the associated implementation plan within 90 days. Those changes, along with necessary conforming cross-reference changes for the remaining six CIP standards, resulted in the version 3 CIP standards. The current phase (Phase II) involves the more complex FERC directives.

The team has been working to revise CIP-002 – Identification of Critical Assets, with the goal of establishing bright line criteria for the identification of critical assets. In November, the SC Executive Committee authorized the team to conduct an abbreviated comment period in parallel with a successive ballot, to support providing stakeholders with the opportunity to provide comment, while also supporting the goal of completing this set of revisions to CIP-002 before the end of December, 2010.

Next Steps

The standards will be submitted to the NERC Board of Trustees for approval.

Ballot Criteria

Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) a two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and non-responses.

Standards Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participated.

For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Exhibit F

Table of CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

CIP-002-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	HIGH	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
R2	HIGH	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.
R3	LOWER	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP-003-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity has documented but not implemented a cyber security policy.	The Responsible Entity has not documented nor implemented a cyber security policy.
R1.1.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.
R1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.3	LOWER	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	The Responsible Entity's senior manager, assigned pursuant to R2, did not annually review **nor** approve its cyber security policy.
R2.	LOWER	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.
R2.1.	LOWER	N/A	N/A	N/A	The senior manager is not identified by name, title, and date of designation.
R2.2.	LOWER	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
R2.3.	LOWER	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
R2.4	LOWER	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
R3.	LOWER	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were documented, **but** were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy (pertaining to CIP 002 through CIP 009), exceptions were not documented, **and** were not authorized by the senior manager or delegate(s).
R3.1.	LOWER	Exceptions to the Responsible Entity's cyber security policy were documented in more than 30 but less than 60 days of being approved by the senior	Exceptions to the Responsible Entity's cyber security policy were documented in 60 or more but less than 90 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 90 or more but less than 120 days of being approved by the senior manager or delegate(s).	Exceptions to the Responsible Entity's cyber security policy were documented in 120 or more days of being approved by the senior manager or delegate(s).

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		manager or delegate(s).			
R3.2.	LOWER	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
R3.3.	LOWER	N/A	N/A	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were reviewed but not approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.	Exceptions to the cyber security policy (pertaining to CIP 002-4 through CIP 009-4) were not reviewed **nor** approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid.
R4.	MEDIUM	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
R4.1.	MEDIUM	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
R4.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
R4.3.	LOWER	N/A	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, documented the assessment results, which included deficiencies identified during the assessment but did not implement a remediation plan.	The Responsible Entity annually assessed adherence to its Critical Cyber Asset information protection program, did not document the assessment results, and did not implement a remediation plan.	The Responsible Entity did not annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, **nor** implement an action plan to remediate deficiencies identified during the assessment.
R5.	LOWER	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5.1.	LOWER	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
R5.1.1.	LOWER	N/A	N/A	The Responsible Entity did identify the personnel by name and title but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name and title nor the information for which they are responsible for authorizing access.
R5.1.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
R5.3.	LOWER	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
R6.	LOWER	The Responsible Entity has established but not documented a change control process OR The Responsible Entity has established but not documented a configuration management process.	The Responsible Entity has established but not documented both a change control process and configuration management process.	The Responsible Entity has not established and documented a change control process OR The Responsible Entity has not established and documented a configuration management process.	The Responsible Entity has not established and documented a change control process AND The Responsible Entity has not established and documented a configuration management process.

CIP-004-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	LOWER	The Responsible Entity established, implemented, and maintained but did not document a security awareness program to	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices.			
R2.	LOWER	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
R2.1.	MEDIUM	At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.	15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.
R2.2.	MEDIUM	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
R2.2.1.	LOWER	N/A	N/A	N/A	N/A
R2.2.2.	LOWER	N/A	N/A	N/A	N/A

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.2.3.	LOWER	N/A	N/A	N/A	N/A
R2.2.4.	LOWER	N/A	N/A	N/A	N/A
R2.3.	LOWER	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.
R3.	MEDIUM	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
R3.1.	LOWER	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) **or** a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
R3.2.	LOWER	N/A	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
R3.3.	LOWER	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4.

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	LOWER	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
R4.1.	LOWER	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
R4.2.	MEDIUM	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-005-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	The Responsible Entity did not document one or more access points to the Electronic Security Perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
R1.1.	MEDIUM	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.2.	MEDIUM	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
R1.3.	MEDIUM	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
R1.4.	MEDIUM	N/A	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.
R1.5.	MEDIUM	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided without four (4) or more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
R1.6.	LOWER	N/A	N/A	The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
				deployed for the access control and monitoring of these access points.	the access control and monitoring of these access points.
R2.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
R2.1.	MEDIUM	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
R2.2.	MEDIUM	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity did not document, individually or by specified grouping, the configuration of those ports and services required for operation and for monitoring Cyber Assets within the Electronic Security Perimeter.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter but did document, individually or by specified grouping, the configuration of those ports and services.	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and did not document, individually or by specified grouping, the configuration of those ports and services.
R2.3.	MEDIUM	N/A	N/A	The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not implement nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
R2.4.	MEDIUM	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5.	LOWER	The required documentation for R2 did not include one of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include two of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include three of the elements described in R2.5.1 through R2.5.4	The required documentation for R2 did not include any of the elements described in R2.5.1 through R2.5.4

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.5.1.	LOWER	N/A	N/A	N/A	N/A
R2.5.2.	LOWER	N/A	N/A	N/A	N/A
R2.5.3.	LOWER	N/A	N/A	N/A	N/A
R2.5.4.	LOWER	N/A	N/A	N/A	N/A
R2.6.	LOWER	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
R3.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring and logging access to access points. OR The Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 5% or more but less than 10% of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 10% or more but less than 15 % of the access points.	The Responsible Entity did not implement electronic or manual processes monitoring and logging at 15% or more of the access points.

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.1.	MEDIUM	The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices. OR Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
R3.2.	MEDIUM	N/A	N/A	Where technically feasible, the Responsible Entity implemented security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses, however the alerts do not provide for appropriate notification to designated response personnel.	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days
R4.	MEDIUM	The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).	The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.
R4.1.	LOWER	N/A	N/A	N/A	N/A
R4.2.	MEDIUM	N/A	N/A	N/A	N/A
R4.3.	MEDIUM	N/A	N/A	N/A	N/A

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.4.	MEDIUM	N/A	N/A	N/A	N/A
R4.5.	MEDIUM	N/A	N/A	N/A	N/A
R5.	LOWER	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005-4.
R5.1.	LOWER	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005-4.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005-4 at least annually.
R5.2.	LOWER	For less than 5% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 5% or more but less than 10% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 10% or more but less than 15% of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	For 15% or more of the applicable changes, the Responsible Entity did not update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
R5.3.	LOWER	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days , but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.

CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval

CIP-006-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
R1.1.	MEDIUM	N/A	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and documented alternative measures to control physical to such Cyber Assets within the Electronic Security Perimeter.
R1.2.	MEDIUM	N/A	The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.	The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.
R1.3	MEDIUM	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
R1.4	MEDIUM	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
R1.5	MEDIUM	N/A	N/A	The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	The Responsible Entity's physical security plan does not address the process for reviewing access authorization requests and the process for revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
R1.6	MEDIUM	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the	The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.	The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.	The Responsible Entity did not include or implement a visitor control program in its physical security plan.

		Physical Security Perimeter.			
R1.6.1	MEDIUM	N/A	N/A	N/A	N/A
R1.6.2	MEDIUM	N/A	N/A	N/A	N/A
R1.7	LOWER	N/A	N/A	The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	The Responsible Entity's physical security plan does not address a process for updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or reconfiguration.
R1.8	LOWER	N/A	N/A	N/A	The Responsible Entity's physical Security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
R2	MEDIUM	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP- 009-4.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided without four (4) or more of the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
R2.1.	MEDIUM	N/A	N/A	N/A	N/A

R2.2.	MEDIUM	N/A	N/A	N/A	N/A
R3	MEDIUM	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) did not reside within an identified Physical Security Perimeter.
R4	MEDIUM	N/A	The Responsible Entity **has implemented but not documented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	The Responsible Entity **has documented but not implemented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	The Responsible Entity has not documented nor implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets..
R5	MEDIUM	N/A	The Responsible Entity has implemented but not documented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the	The Responsible Entity has documented but not implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel	The Responsible Entity has not documented nor implemented the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

			following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4.
R6	LOWER	The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify	The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, **but** has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week..	The Responsible Entity has documented but not implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	The Responsible Entity has not implemented nor documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

		individuals and the time of access twenty-four hours a day, seven days a week.			
R7	LOWER	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
R8	MEDIUM	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.
R8.1	MEDIUM	N/A	N/A	N/A	N/A
R8.2	LOWER	N/A	N/A	N/A	N/A
R8.3	LOWER	N/A	N/A	N/A	N/A

CIP-007-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	MEDIUM	N/A	The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, **but did not document** that testing is performed as required in R1.2.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.	The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1, AND The Responsible Entity did not document that testing was performed as required in R1.2 AND

			OR The Responsible Entity did not document the test results as required in R1.3.		The Responsible Entity did not document the test results as required in R1.3.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R2.	MEDIUM	N/A	The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.	The Responsible Entity did not establish (implement) nor document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R2.1.	MEDIUM	The Responsible Entity enabled ports and services not required for normal and emergency operations on at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity enabled ports and services not required for normal and emergency operations on 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.2.	MEDIUM	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).
R2.3.	MEDIUM	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk exposure.

R3.	LOWER	The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not establish (implement) nor document, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
R3.1.	LOWER	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in more than 30 but less than 60 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 60 or more but less than 90 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 90 or more but less than 120 calendar days after the availability of the patches and upgrades.	The Responsible Entity documented the assessment of security patches and security upgrades for applicability as required in Requirement R3 in 120 calendar days or more after the availability of the patches and upgrades.
R3.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure.
R4.	MEDIUM	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).

		tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).		
R4.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
R4.2.	MEDIUM	The Responsible Entity, as technically feasible, documented and implemented a process for the update of anti-virus and malware prevention "signatures.", but the process did not address testing and installation of the signatures.	The Responsible Entity, as technically feasible, did not document but implemented a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, documented but did not implement a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention "signatures."	The Responsible Entity, as technically feasible, did not document nor implement a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
R5.	LOWER	N/A	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
R5.1.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
R5.1.1.	LOWER	At least one user account but less than 1% of user accounts implemented by the Responsible Entity, were not approved by designated personnel.	One (1) % or more of user accounts but less than 3% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Three (3) % or more of user accounts but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	Five (5) % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
R5.1.2.	LOWER	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.

			access activity, however the logs do not contain activity for a minimum of 90 days.		
R5.1.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.
R5.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
R5.2.1.	MEDIUM	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
R5.2.2.	LOWER	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
R5.2.3.	MEDIUM	N/A	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 1 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts, but is missing 2 of the following 3 items: a) limits access to only those with authorization, b) has an audit trail of the account use (automated or manual), c) has specified steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	Where such accounts must be shared, the Responsible Entity does not have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
R5.3.	LOWER	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires but does not use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity does not require nor use passwords as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.

R5.3.1.	LOWER	N/A	N/A	N/A	N/A
R5.3.2.	LOWER	N/A	N/A	N/A	N/A
R5.3.3.	MEDIUM	N/A	N/A	N/A	N/A
R6.	LOWER	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for at least one but less than 5% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not implement automated tools or organizational process controls to monitor system events that are related to cyber security for 5% or more but less than 10% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 10% or more but less than 15% of Cyber Assets inside the Electronic Security Perimeter(s).	The Responsible Entity did not implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security for 15% or more of Cyber Assets inside the Electronic Security Perimeter(s).
R6.1.	MEDIUM	N/A	The Responsible Entity implemented but did not document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity documented but did not implement the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity did not implement nor document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
R6.2.	MEDIUM	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
R6.3.	MEDIUM	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.
R6.4.	LOWER	The Responsible Entity retained the logs specified in Requirement R6, for at least 60 days, but less than 90 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least 30 days, but less than 60 days.	The Responsible Entity retained the logs specified in Requirement R6, for at least one day, but less than 30 days.	The Responsible Entity did not retain any logs specified in Requirement R6.

R6.5.	LOWER	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
R7.	LOWER	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP- 005-4 **but** did not maintain records as specified in R7.3.	The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address disposal as specified in R7.1.	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.
R7.1.	LOWER	N/A	N/A	N/A	N/A
R7.2.	LOWER	N/A	N/A	N/A	N/A
R7.3.	LOWER	N/A	N/A	N/A	N/A
R8	LOWER	The Responsible Entity performed at least annually a Vulnerability Assessment that included 95% or more but less than 100% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included 90% or more but less than 95% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment that included more than 85% but less than 90% of Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of Cyber Assets within the Electronic Security Perimeter. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
R8.1.	LOWER	N/A	N/A	N/A	N/A
R8.2.	MEDIUM	N/A	N/A	N/A	N/A

R8.3.	MEDIUM	N/A	N/A	N/A	N/A
R8.4.	MEDIUM	N/A	N/A	N/A	N/A
R9	LOWER	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **nor** were changes resulting from modifications to the systems or controls documented within thirty calendar days of the change being completed.

CIP-008-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	LOWER	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.	The Responsible Entity has developed a Cyber Security Incident response plan but the plan does not address one or more of the subrequirements R1.1 through R1.6.	The Responsible Entity has not developed a Cyber Security Incident response plan or has not implemented the plan in response to a Cyber Security Incident.
R1.1.	LOWER	N/A	N/A	N/A	N/A
R1.2.	LOWER	N/A	N/A	N/A	N/A
R1.3.	LOWER	N/A	N/A	N/A	N/A
R1.4.	LOWER	N/A	N/A	N/A	N/A

R1.5.	LOWER	N/A	N/A	N/A	N/A
R1.6.	LOWER	N/A	N/A	N/A	N/A
R2	LOWER	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for two but less than three calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than two calendar years.	The Responsible Entity has kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for less than one calendar year.	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1.

CIP-009-4

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	MEDIUM	N/A	The Responsible Entity has not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-4 R1.1 **or** R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-4 R1.1 **and** R1.2.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A
R1.2.	MEDIUM	N/A	N/A	N/A	N/A
R2	LOWER	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
R3	LOWER	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR

		from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 30 but less than or equal to 120 calendar days of the change.	updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.	the change.	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 180 calendar days of the change.
R4	LOWER	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
R5	LOWER	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.